


3 1761 11648387 6



Digitized by the Internet Archive
in 2023 with funding from
University of Toronto

<https://archive.org/details/31761116483876>

CAI
ND 800
-516

Government
Publications 15



ANNUAL REPORT

of the Communications Security
Establishment Commissioner



Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station 'B'
Ottawa, Ontario
K1P 5R5

Tel: (613) 992-3044
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 1997
ISBN 0-662-62910-8
Cat. No. JS95-1997
ISSN 1206-7490

Communications Security
Establishment Commissioner



The Honourable Claude Bisson

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Claude Bisson

April 11, 1997

The Honourable Douglas Young
Minister of National Defence and
Minister of Veterans Affairs
101 Colonel By Drive
Ottawa, Ontario
K1A 0K2

Dear Mr. Young:

Pursuant to paragraph (b) of Order in Council P.C. 1996-899
appointing me Communications Security Establishment Commissioner, I am
pleased to submit to you my first annual report on my activities and findings from
June 19, 1996 to March 31, 1997, for your submission to Parliament.

Yours sincerely,

A handwritten signature in black ink that reads "Claude Bisson". The signature is fluid and cursive, with the first letter of "Claude" being a large, stylized "C".

The Honorable Claude Bisson



TABLE OF CONTENTS

Preface	1
My Appointment and Mandate	2
Origins of the Communications Security Establishment (CSE)	3
Mandate of CSE	5
Calls for Review and Accountability	6
First-Year Review	7
• Activities	7
• Findings	10
• Limitations	12
Budget and Staff	12
Next Steps	12
Appendix	15
• Order in Council P.C. 1996-899	15

Preface

The Government of Canada relies on information and intelligence obtained through a variety of means and from a wide range of sources as part of its efforts to protect the country's assets and interests. Canada's ability to meet its many international obligations, for example, in peacekeeping efforts and the fight against terrorism, are assisted by intelligence collection, analysis and dissemination.

During the early months following my appointment, it became apparent to me that both the collectors and users of intelligence in Canada share the view that the end of the Cold War gave rise to new and complex challenges. Indeed, information and intelligence collected throughout the '90s reveal a diversification of, and an increase in, threats to the security interests of many nations, including Canada. Political, social, and economic volatility and, in some instances, instability, together with the disappearance of a common foe, threaten defences and security globally.

The free movement of peoples and materiel has resulted in an increase in the threat of terrorism. It has also raised global concerns regarding the proliferation and ready availability of weapons of mass destruction, and contributed to the spread of organized criminal activity. Global economic and technological competition also play a role in this developing mosaic, and the number of potential and known targets--persons and organizations--has grown.

In order to meet these challenges, the security and intelligence components of the Government of Canada have played a vital role in the collection, analysis and dissemination of information and intelligence on issues that affect national interests. As a member of Canada's security and intelligence community, the Communications Security Establishment (CSE) contributes to these efforts through the delivery of its mandated programs,



commonly known as foreign signals intelligence (SIGINT) and information technology security (ITS).

I believe, however, that the citizens of this country have a justifiable expectation that agencies that must conduct much of their business in secret do so in compliance with the laws of Canada. Providing this assurance in respect of CSE is my responsibility.

My Appointment and Mandate

On June 19, 1996, the Minister of National Defence announced my appointment to the position of Communications Security Establishment Commissioner, pursuant to Part II of the *Inquiries Act*, for a term of three years. I serve in this capacity on a part-time basis, and my mandate, which is established by Order in Council, is as follows:

- to review the activities of CSE for the purpose of determining whether they are in compliance with the law,
- to advise the Minister of National Defence and the Attorney General of Canada of any activity of CSE that I believe may not be in compliance with the law,
- not to review issues for which other avenues of redress are established by statute,
- to submit to the Minister a report containing classified information when I consider it advisable,
- to submit to the Minister an annual report in both official languages on my activities and findings for tabling in Parliament.

On May 9, 1996 I retired as a judge of the Quebec Court of Appeal after more than twenty-seven years on the bench. Upon accepting my appointment as CSE Commissioner, I became immersed in aspects

of Canada's security and intelligence community in general and CSE in particular. In this regard, the origins of CSE are worth noting.

Origins of CSE

CSE's role in the collection of SIGINT spans several decades. In 1925, under the direction of the British Royal Navy (the Admiralty), the Royal Canadian Navy established Canada's first high-frequency direction-finding (HF/DF) station at the Esquimalt naval base on Vancouver Island. In subsequent years, a series of stations were set up across Canada, and HF/DF intercepts served as a means of assisting the Admiralty to track ships in the Pacific Ocean; the Admiralty already had stations covering the Atlantic.

Canada's assistance to Britain grew during the late '20 and '30s. At that time, SIGINT activities encompassed not only locating and monitoring foreign transmissions via HF/DF, but expanded to include the monitoring of wireless intercepts by Canada's Army and by the Department of Transport's Wireless Service. With the onset of World War II, Britain sought Canada's continued participation in providing direction-finding and raw intercept information which was used, for example, by the British Royal Navy and Britain's Radio Security Service.

As the war progressed and as the volume of raw data increased, Canada's need for its own code and cipher-breaking capabilities was discussed and debated among various government officials, including those in Canada's military services, the Department of External Affairs (DEA), the Royal Canadian Mounted Police (RCMP), and the National Research Council. During this period of debate, US and UK allies expressed their view that Canada ought to become an active participant and develop its own expertise in this area.

In 1941, at the urging of the Department of External Affairs, the government established a national signals intelligence bureau known as the Examination Unit (XU). The XU was located in the National Research Council and included participation from the RCMP, DEA, and the three military services. Under XU coordination, raw intercepts and decrypted traffic were used by Canadian intelligence consumers, and were relayed to and from SIGINT allies in Britain and the United States. Intercepted traffic included messages from the Soviet Union, Germany, Italy, South America and Asia. By war's end, the XU was renamed the Joint Discrimination Unit and was a fully-functioning signals intelligence service.

Deliberations commenced in 1944 (principally among DEA, Army and Navy officials) to determine the need for, and the structure of, a possible post-war organization, as well as the role it would play in meeting the intelligence requirements of the government of the day. It was at this juncture that the two programs that evolved into CSE's current mandate began to take shape.

First, it was determined that continued signals collection was necessary for the protection of Canada's foreign and defence interests. The government's decision was influenced by requests for continuing intelligence assistance from the United States and Britain, and by Soviet defector Igor Gouzenko's identification of Soviet intelligence activities in Canada and the United States. This gave birth to CSE's SIGINT mandate.

Second, it was clear that federal government departments and agencies now required advice and assistance to protect classified information from interception by unfriendly parties. This led to the creation of CSE's defensive mandate, then known as Communications-Electronic Security (COMSEC), and now referred to as Information Technology Security (ITS).

In 1946, this new peacetime national cryptologic organization was established by Order in Council and renamed the Communications Branch, National Research Council (CBNRC), with responsibility for both SIGINT and COMSEC. In 1975, an Order in Council transferred CBNRC to the Department of National Defence and named the Minister responsible for designated activities pursuant to section 4 of the *National Defence Act*. At the same time, the organization was renamed the Communications Security Establishment.

Through CSE, Canada has maintained collaborative relationships with some of its close and long-standing allies in exchanging foreign intelligence and sharing sensitive information technology security. The allies are the United States, the United Kingdom, Australia and New Zealand, and each has an organization that is analogous to CSE.

Mandate of CSE

Today CSE is Canada's national cryptologic agency. In its SIGINT capacity, CSE collects and analyzes foreign radio, radar and other electronic emissions; it is assisted in this activity by the Canadian Forces Supplementary Radio System (CFSRS), a component of the Canadian Forces, which operates from a number of stations around the country.

Through the provision of signals intelligence, CSE contributes to the government's foreign intelligence program. Foreign intelligence refers to information or intelligence about the capabilities, intentions or activities of foreign states, corporations, or persons in relation to the defence of Canada or the conduct of its international affairs. It may include information of a political, economic, military, scientific or social nature that could have security implications.

Through its ITS program, CSE provides technical advice, guidance and service on the means of assuring government telecommunications security

Calls for Review and Accountability

and on aspects of electronic data processing security. CSE's objective is to help the federal government achieve an appropriate level of security for its telecommunications and automated information systems. CSE meets this objective by providing departments with both the means and advice to ensure the protection of classified and designated information. In this capacity, the service provided by CSE is intended to prevent access to sensitive information carried on government telephone and computer systems by any unauthorized person or organization, and to protect the integrity and availability of government information.

The timing of my appointment in June 1996 was opportune for a number of reasons. First, the following month, the Privacy Commissioner issued a report to the Chief of CSE detailing the findings of a compliance audit he had recently completed. The audit report is a classified document; however, reference to the audit was made in the Privacy Commissioner's public annual report. He observed that for a number of reasons, including the lack of a legislative framework, the CSE audit had proven to be a complex undertaking. In particular, he noted, "...in the midst of the audit, there were several public allegations that CSE was gathering data about Canadians and monitoring their legitimate political activities."

The Privacy Commissioner reviewed a representative sampling of SIGINT data and reports and concluded that CSE collects only information that serves the government's established foreign intelligence criteria. No evidence was found to support any allegations that CSE targets Canadians or monitors their communications. CSE uses strict procedures to minimize the possibility that information about Canadians is captured inadvertently. The Privacy Commissioner concluded, to the extent that it could be established through his audit, that CSE

operates in compliance with the *Privacy Act* and the principles of fair information practices. However, he recommended the enactment of enabling legislation, describing CSE's mandate, powers, activities and responsibilities.

In November 1996, the Auditor General of Canada tabled his report, *The Canadian Intelligence Community--Control and Accountability*. The report, which offered a *tour d'horizon* of the community, revealed that comprehensive policies and procedures exist at CSE to guide operational activities and that operations related to safeguarding the privacy of Canadians are reviewed annually. It identified a need for continuing progress, however, in the areas of control and accountability. In this regard, the report made reference to the establishment and mandate of my office, and its existence as an external mechanism to review CSE's foreign signals collection activities.

The Auditor General's report expressed the view that the activities of my office should increase the scope for informed parliamentary scrutiny and debate, including the question of whether it would be in the public interest for Parliament to consider establishing a statutory basis for CSE. The report concluded with a call to the government to consider the advantages of an appropriate legislative framework.

First-Year Review

Activities

My first tasks following my appointment revolved around establishing and staffing my office. With the support of officials at the Privy Council Office and the Department of National Defence, my office was soon centrally located in downtown Ottawa. However, modifications were required to upgrade the premises to meet the standard required for handling and storing classified material. By September, my office was established and fully operational.

At CSE headquarters two offices were also made available. This arrangement facilitated my and my staff's ability to obtain and examine classified and sensitive information without having to introduce complex and cumbersome procedures to transfer documents to my office downtown.

As I launched my review function, I was cognizant that I was not charting new territory; review mechanisms have been enshrined in legislation and active within sectors of the intelligence community in Canada and abroad for years. I was able to benefit from the experiences of these review bodies.

For example, both the Inspector General of CSIS and the Security Intelligence Review Committee (SIRC) came into being following the creation of CSIS and pursuant to the *Canadian Security Intelligence Service Act* in 1984. I met with the current Inspector General and the Chair of SIRC, who were generous with their time. I was also pleased to have the opportunity to meet and discuss review mandates with the Australian Inspector General of Intelligence and Security, during his visit to Canada in September.

An extensive series of meetings occupied my time and that of my staff during the autumn months. There were detailed discussions at CSE regarding its mandate and operations and at Leirtrim, Ontario, on the Canadian Forces Supplementary Radio System. There were also discussions with the Director of CSIS and his officials, and with the Senior Adviser and Coordinator of Security and Intelligence, Privy Council Office, and his officials, whose information allowed me to gain an appreciation of the broader aspects of the community.

I had an opportunity to meet with the Auditor General of Canada and the Privacy Commissioner to discuss their respective reports. In addition, the Deputy Minister of Justice, and his officials

provided valuable information regarding the role Justice plays in the security and intelligence community in general, and at CSE in particular.

There are obviously limitations to what I am able to report about CSE and its operations. It functions in a highly complex environment and must keep abreast of the rapid pace of changing technology. However, my staff and I had unfettered access, and we were given all the information and documentation we requested. I benefitted from a broad overview of all CSE activities, some of which I later examined in greater detail.

During this initial period of review, I focussed my attention on the control and accountability measures currently in place at CSE. In doing so I drew considerable value from the discussion of these measures in the report of the Auditor General. Specifically, I concur with the Auditor General's assessment of the important legal function exercised by the Department of Justice. Legal counsel assigned to CSE from Justice are members of CSE's senior management team and an integral part of the operational decision-making process. They are fully cleared for, and have access to, all information. On a continuing basis, they provide advice on the legality of activities under consideration and of existing operations, to determine whether they are in accordance with the law.

As is the case with most federal departments and agencies, CSE is also subject to external review. Its activities must withstand the independent scrutiny of the courts, the Canadian Human Rights Commission, the Privacy Commissioner, the Information Commissioner, the Commissioner of Official Languages and, of course, the Auditor General of Canada. As noted in the Auditor General's report, however, these review bodies can bring to bear only their specific mandates in carrying out their work.

Control and accountability at CSE are equally evident at the ministerial level, since the Minister of National Defence is answerable in Parliament for all CSE activities. The Minister must approve capital spending and major spending recommendations made to Treasury Board. The Minister also approves key policy initiatives and is responsible for CSE issues in Cabinet.

Two deputy ministers, the Security and Intelligence Coordinator in the Privy Council Office and the Deputy Minister of National Defence, are responsible for ensuring that the Minister is fully informed of CSE's activities. The Security and Intelligence Coordinator is accountable for CSE's policy and operations, and the Deputy Minister of National Defence is accountable for administrative matters. CSE responds to foreign intelligence needs approved by Cabinet and to specific departmental requests or event-driven intelligence needs of the government.

Findings

Based on the results of my own review and analysis, I am of the opinion that CSE has acted lawfully in the performance of its mandated activities during the period under review. I am also satisfied that CSE has not targeted Canadian citizens or permanent residents. In this regard, my opinion has been reinforced by the reports of the Privacy Commissioner and the Auditor General of Canada, referred to earlier.

Paragraph (c) of the Order in Council appointing me CSE Commissioner authorizes me to submit a report containing classified information to the Minister of National Defence any time that I consider it advisable. In March 1997, I submitted a report to the Minister, bringing to his attention certain procedures that, in my opinion, required

some review and refinement. The issues I raised were resolved to the satisfaction of all parties. Unlawful activity on the part of CSE was not the subject of this report.

A topic of continuing discussion is the issue of enabling legislation for CSE. An early reference to this issue appeared in the form of a recommendation in the Report of the Special Parliamentary Committee on the Review of the *CSIS Act*, which was tabled in September 1990. Subsequently, the matter was raised on a number of occasions, most recently by the Privacy Commissioner and the Auditor General.

There is no doubt that CSE occupies a unique position within the structure of the government of Canada, and not only because of its mandate. It does not have a legislative framework, nor does its name appear in the schedules of the *Financial Administration Act*. Yet, in my opinion, a number of policy issues should be examined or revisited before any decision is taken to begin legislative drafting. These include the scope and structure of a legislative framework, as well as limitations and related policy issues; control and accountability issues; and the scope and structure of enshrined review mechanisms.

Despite recent calls for legislation for CSE, I do not intend to express any further opinions on this topic until I have had time to study the matter further. However, I cannot help but note the remarkable window of opportunity these calls present given the new and complex challenges in the security and intelligence landscape, and the rapid pace of technological change, both of which go to the heart of CSE's mandate.

Limitations

Under the terms and conditions of the Order in Council appointing me Commissioner, I am precluded from reviewing issues for which other avenues of redress are established by statute, and I am able to review only those issues that relate directly to the mandate of CSE. This does not seem unreasonable to me given the focus of my mandate, and the fact that my office was never intended to be a court of last resort. Also, as I indicated when I was named Commissioner, I do not intend to review incidents that predate my appointment.

Despite the clarity of my mandate, one limitation may prove problematic in the longer term. While I am authorized to review any allegation concerning certain activities of CSE, I cannot inform individual complainants of the fact of my review or my findings. This may lead to dashed expectations, given the purpose of my office. However, some comfort should be drawn from the general assurance I can provide in this report of the lawfulness of CSE's activities.

Budget and Staff

I requested and was allocated an annual budget of \$500,000, including salaries for three full-time positions. In addition, rather than establishing a larger staff complement, I have opted to secure expert services as I require them on a contractual basis.

I am able to report that during the first ten-month period of operation, my office was established and I discharged my mandated activities within budget.

Next Steps

Obviously, it was not possible to review all aspects of CSE's complex operations within the first ten months of my mandate. Therefore, during the next year, my main priority is to continue reviewing the activities of CSE, examining some of them in greater depth, and to issue periodic reports to the Minister of National Defence as appropriate. I also anticipate further discussions arising from the limitation I referred to previously.

In closing, I believe it is important to acknowledge that the government will continue to require CSE to deliver its foreign intelligence and information security programs even as the provisions of a constituent act are under debate. In the meantime, the issue of legislation remains of abiding interest to me, and I anticipate becoming involved in the discussions that will no doubt ensue.



CANADA

PRIVY COUNCIL • CONSEIL PRIVÉ

P.C. 1996-899

June 19, 1996

His Excellency the Governor General in Council, on the recommendation of the Minister of National Defence, pursuant to Part II of the *Inquiries Act*, hereby authorizes the Minister of National Defence ("Minister"):

- (a) to appoint the Honourable Claude Bisson of Montreal, Quebec, for a period of three years, as a commissioner ("Commissioner") to review the activities of the Communications Security Establishment ("CSE") for the purpose of determining whether those activities are in compliance with the law;
- (b) to direct the Commissioner to submit to the Minister, once each year and in both official languages, a report on the Commissioner's activities and findings that are not of a classified nature, which report the Minister will table in Parliament;
- (c) to authorize the Commissioner, at any time the Commissioner considers it advisable, to submit a report containing classified information to the Minister;
- (d) to direct the Commissioner to advise the Minister and the Attorney General of Canada of any activity of CSE that the Commissioner believes may not be in compliance with the law;
- (e) to direct the Commissioner not to review issues for which other avenues of redress are established by statute;

.../2

- 2 -

(f) to require that the Commissioner and all persons engaged on his behalf take an oath of secrecy and comply with all applicable government security requirements;

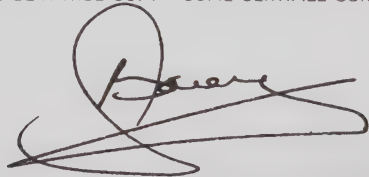
(g) to direct the Commissioner, before submission of any report to the Minister, to consult with the Deputy Clerk, Security and Intelligence, and Counsel at the Privy Council Office for the purpose of ensuring compliance with all security requirements and preservation of the secrecy of sources of security and intelligence information and of the security of information provided to Canada in confidence by other nations;

(h) to authorize the Commissioner to engage the services of such staff and technical advisors as he considers necessary to assist him in his review, at such rates of remuneration and reimbursement as may be approved by the Treasury Board;

(i) to fix the remuneration of the Commissioner at the per diem rate set out in the schedule hereto, which rate is within the range of \$400 to \$500; and

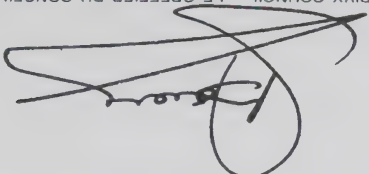
(j) to authorize that the Commissioner be reimbursed for his actual transportation expenses and a non-accountable living allowance of up to \$175 per diem while in travel status away from his normal place of residence in connection with the conduct of this review.

CERTIFIED TO BE A TRUE COPY - COPIE CERTIFIÉE CONFORME

A handwritten signature in dark ink, appearing to be 'D. Gaudet', is written over a large, stylized circular flourish or seal.

CLERK OF THE PRIVY COUNCIL - LE GREFFIER DU CONSEIL PRIVÉ

CLERK OF THE PRIVY COUNCIL - LE GREFFIER DU CONSEIL PRIVÉ



CERTIFIED TO BE A TRUE COPY - COPIE CERTIFIÉE CONFORME

j) à autoriser le remboursement des frais de transports réels du commissaire ainsi qu'une allocation de subsistance non à justifier allant jusqu'à 175 \$ par jour lors de son déplacement à l'extérieur de son lieu de résidence habituel dans l'exercice des fonctions de cette enquête.

i) à fixer la rémunération du commissaire au taux journalier établi dans l'annexe ci-jointe, lequel taux se situe dans l'échelle de 400 \$ à 500 \$;

h) à autoriser le commissaire à retenir les services des experts et du personnel qu'il juge nécessaires pour l'assister dans son enquête, aux taux de rémunération que peut approuver le Conseil du Trésor;

g) à ordonner au commissaire, avant la présentation de tout rapport au ministre, de consulter le sous-greffier, sécurité et renseignement et conseiller juridique au Bureau du Conseil privé en vue de veiller à ce que toutes les exigences visant la sécurité soient respectées et que la confidentialité des sources de sécurité et de renseignements secrets et la sécurité de l'information fournie au Canada par d'autres nations à titre confidentiel soit protégée;

f) à exiger que le commissaire et toutes les personnes engagées pour son compte prononcent un serment de discrétion et se conforment à toutes les exigences du gouvernement applicables au secret;



Sur recommandation du ministre de la Défense nationale et en vertu de la partie II de la Loi sur les enquêtes, son Excellence le Gouverneur général en conseil autorise le ministre de la Défense nationale (ci-après appelé le « ministre ») :

a) à nommer l'honorable Claude Bissson, de Montréal (Québec), pour une période de trois ans, commissaire pour faire enquête sur les activités du Centre de la sécurité des télécommunications (« CST ») en vue de déterminer si ces activités sont conformes à la loi;

b) à ordonner au commissaire de présenter au ministre, une fois l'an et dans les deux langues officielles, un rapport sur ses activités et ses constatations qui ne sont pas de nature classifiée, lequel rapport sera déposé par le ministre auprès du Parlement;

c) à autoriser le commissaire à soumettre au ministre tout rapport classifié, aux moments où il le juge indiqué;

d) à ordonner au commissaire d'aviser le ministre et le procureur général du Canada au sujet de toute activité du CST qu'il estime ne pas être conforme à la loi;

e) à ordonner au commissaire de ne pas examiner les questions pour lesquelles il existe d'autres recours statutaires;

Prochaines étapes

Au cours de nos dix premiers mois d'activité, mon bureau a été mis sur pied et je me suis acquitté de mon mandat dans les limites de ce budget.

Il ne m'a manifestement pas été possible d'examiner tous les aspects des opérations complexes du CST pendant les dix premiers mois de mon mandat. Au cours de l'année prochaine, ma principale priorité consistera par conséquent à continuer de passer en revue les activités du CST, à en examiner certaines plus à fond, et à communiquer des rapports périodiques au ministre de la Défense nationale, selon les besoins. Je prévois par ailleurs que la limite à laquelle j'ai fait allusion plus haut donnera lieu à de nouvelles discussions.

Pour conclure, j'estime important de reconnaître que le gouvernement continuera d'avoir besoin du CST pour exécuter ses programmes de renseignement étranger et de sécurité de l'information même pendant qu'on débatera des dispositions d'une loi constitutive. Dans l'intervalle, cette question ne cesse de m'intéresser, et je compte prendre part aux discussions qui s'ensuivront sans aucun doute.

Malgré les demandes récentes visant l'adoption d'une mesure législative pour régir le CST, je n'ai pas l'intention d'exprimer d'autre opinion sur le sujet avant d'avoir eu le temps d'étudier la question plus à fond. Toutefois, je ne peux m'empêcher de constater l'occasion remarquable que présentent ces demandes, compte tenu des défis nouveaux et complexes à relever dans le domaine de la sécurité et du renseignement et du rythme rapide de l'évolution technologique, deux faits qui touchent au coeur même du mandat du CST.

Les conditions énoncées dans le décret relatif à ma nomination m'empêchent d'examiner les questions pour lesquelles il existe d'autres recours prévus par la loi; je peux seulement examiner celles qui se rapportent directement au mandat du CST. Cela ne m'apparaît pas déraisonnable, compte tenu de l'objet de mon mandat et du fait qu'il n'a jamais été question de faire de mon bureau un tribunal de dernier ressort. Par ailleurs, comme je l'ai signalé lors de ma nomination, je n'entends pas examiner d'incidents survenus antérieurement.

Malgré la clarté de mon mandat, une de ses limites pourrait poser un problème à long terme. En effet, je suis autorisé à examiner les allégations relatives à certaines activités du CST, mais je ne peux informer les plaignants de l'exécution de mon examen, ni de mes constatations. Cela risque de frustrer certaines attentes, étant donné le but de mon poste. Cependant, la garantie générale de légalité des activités du CST que je peux donner dans le présent rapport devrait être rassurante.

J'ai demandé et obtenu un budget annuel de 500 000 \$ dans lequel sont compris les traitements de trois employés à temps plein. Par ailleurs, au lieu de me doter d'un personnel plus nombreux, j'ai choisi de retenir les services d'experts au fur et à mesure des besoins.

Limites

Budget et personnel

cet égard, mon opinion a été renforcée par les rapports du commissaire à la protection de la vie privée et du vérificateur général du Canada, dont j'ai fait mention plus haut.

L'alinéa c) du décret relatif à ma nomination au poste de commissaire du CST m'autorise à présenter au ministre de la Défense nationale des rapports renfermant des renseignements classifiés lorsque je le juge à propos. En mars 1997, j'ai présenté au Ministre un rapport dans lequel j'attirais son attention sur certaines procédures qui, à mon avis, devaient être examinées et améliorées. Les questions que j'ai soulevées ont été réglées à la satisfaction de toutes les parties. Ce rapport n'avait pas trait à des activités illégales de la part du CST.

L'adoption d'une loi habilitante pour régir le CST est un sujet de discussion qui revient régulièrement. Cette question s'est d'abord présentée sous la forme d'une recommandation contenue dans le rapport du comité parlementaire spécial chargé de l'examen de la *Loi sur le SCRS*, qui a été déposé en septembre 1990. Elle a ensuite été soulevée à diverses reprises, notamment tout dernièrement, par le commissaire à la protection de la vie privée et par le vérificateur général.

Il n'y a pas de doute que le CST occupe une place unique dans la structure du gouvernement du Canada et ce, pas seulement en raison de son mandat. Il ne possède pas de cadre législatif, et son nom ne figure pas non plus dans les annexes de la *Loi sur la gestion des finances publiques*. Il faudrait néanmoins, à mon avis, examiner ou revoir certaines questions de politique avant de prendre quelque décision que ce soit touchant la rédaction d'une loi. Figurent au nombre de ces questions la portée et la structure du cadre législatif, de même que ses limites et les aspects stratégiques connexes; les questions de contrôle et de responsabilisation; la portée et la structure des mécanismes d'examen qui seraient prévus dans la loi.

Commission canadienne des droits de la personne, du commissaire à la protection de la vie privée, du commissaire à l'information, du commissaire aux langues officielles et, bien entendu, du vérificateur général du Canada. Comme ce dernier le mentionne dans son rapport, toutefois, ces organismes d'examen sont limités dans leur travail par leurs mandats particuliers.

Au CST, le contrôle et l'obligation de rendre compte sont également manifestes au palier ministériel, car le ministre de la Défense nationale est comptable de toutes les activités du CST devant le Parlement. Il doit approuver les dépenses en capital de l'organisme et les recommandations de dépenses importantes qu'il fait au Conseil du Trésor. Il approuve en outre ses grandes initiatives de politique et est responsable, devant le cabinet, de toutes les questions relatives au CST.

Il incombe à deux sous-ministres, soit le coordonnateur de la sécurité et du renseignement du Bureau du Conseil privé et le sous-ministre de la Défense nationale, de veiller à ce que le Ministre soit pleinement tenu au courant des activités du CST. Le coordonnateur de la sécurité et du renseignement a la responsabilité de la politique et des activités du CST, et le sous-ministre de la Défense nationale s'occupe des questions administratives. Le CST répond aux besoins de renseignements étranger approuvés par le cabinet et à des demandes précises des ministères ou à des besoins de renseignements du gouvernement liés à des événements particuliers.

Constatations

Les résultats de mon examen et de mon analyse m'amènent à conclure que le CST a agi légalement dans la poursuite des activités prévues par son mandat au cours de la période étudiée. Je suis par ailleurs convaincu qu'il n'a pas ciblé de citoyens canadiens ni de résidents permanents du Canada. À

J'ai eu l'occasion de rencontrer le vérificateur général du Canada et le commissaire à la protection de la vie privée pour discuter de leurs rapports respectifs. En outre, le sous-ministre de la Justice et ses fonctionnaires m'ont fourni des renseignements précieux sur le rôle joué par le ministère de la Justice au sein de la communauté de la sécurité et du renseignement en général et au CST en particulier.

Il y a manifestement des limites à ce que je peux divulguer au sujet du CST et de ses opérations. Cet organisme exerce son activité dans un cadre extrêmement complexe et doit suivre le rythme rapide de l'évolution technologique. Néanmoins, mon personnel et moi-même avons eu librement accès à tous les renseignements et documents voulus, qui nous ont été remis sur demande. J'ai obtenu une vue d'ensemble étendue de toutes les activités du CST et j'en ai examiné certaines de façon plus détaillée par la suite.

Au cours de cette période initiale d'examen, j'ai concentré mon attention sur les mesures de contrôle et de responsabilisation actuellement en place au CST. La discussion de ces mesures contenue dans le rapport du vérificateur général m'a été extrêmement utile à cet égard. Je partage notamment le point de vue de ce dernier concernant l'importante fonction juridique exercée par le ministère de la Justice. Les conseillers juridiques affectés par ce ministère au CST font partie de la haute direction de l'organisme et participent aux décisions relatives à ses activités. Ils possèdent l'autorisation sécuritaire voulue pour avoir accès à tous ses renseignements. Ils donnent en permanence des avis sur la légalité des activités envisagées et des opérations en cours afin de déterminer leur conformité avec la loi.

Comme la plupart des ministères et organismes fédéraux, le CST est également assujéti à un examen externe. Ses activités doivent résister à l'examen indépendant des tribunaux, de la

Deux bureaux ont également été mis à ma disposition au siège central du CST. Mon personnel et moi-même avons ainsi pu obtenir et examiner plus facilement des renseignements classifiés et délicats sans devoir nous encombrer de toutes sortes de formalités pour transférer des documents à mon bureau du centre-ville.

Au moment d'entreprendre mon travail d'examen, j'étais conscient de ne pas faire oeuvre de pionnier : des mécanismes d'examen étaient en effet prévus par la loi et appliqués dans divers secteurs de la communauté du renseignement au Canada et à l'étranger depuis des années. J'ai donc pu profiter de l'expérience de ces organismes.

Par exemple, le poste d'inspecteur général du SCRS et le Comité de surveillance des activités du renseignement de sécurité (CSARS) ont tous deux vu le jour après la création du SCRS et conformément à la *Loi sur le Service canadien du renseignement de sécurité*, en 1984. J'ai rencontré l'inspecteur général actuel ainsi que la présidente du CSARS, qui m'ont donné généreusement de leur temps. J'ai en outre eu le plaisir de rencontrer l'inspecteur général de la sécurité et du renseignement d'Australie, avec qui j'ai discuté de mandats d'examen lors de sa visite au Canada, en septembre dernier.

Au cours de l'automne, mon personnel et moi-même avons été mobilisés par toute une série de réunions. Nous avons participé à des discussions détaillées, au CST, touchant son mandat et ses activités, et à Leitrin (Ontario), au sujet du Réseau radio supplémentaire des Forces canadiennes. Nous avons également eu des entretiens avec le directeur du SCRS et ses fonctionnaires, et avec le conseiller supérieur et coordonnateur de la sécurité et du renseignement au Bureau du Conseil privé et ses fonctionnaires; les renseignements ainsi obtenus m'ont permis de comprendre les aspects plus larges de la communauté.

Revue de la première année Activités

les principes d'équité en matière de pratiques d'in-
formation. Il a toutefois recommandé l'adoption
d'une loi habilitante énonçant le mandat, les pou-
voirs, les activités et les responsabilités du CST.

En novembre 1996, le vérificateur général du
Canada a déposé son rapport intitulé *La commu-
nauté canadienne du renseignement — Le contrôle
et la responsabilisation*, dans lequel il fait un tour
d'horizon de cette communauté. Ce rapport révèle
qu'il existe au CST des politiques et des procédures
détaillées destinées à guider ses opérations et que
les mesures ayant trait à la protection de la vie
privée des Canadiens sont examinées chaque année.
Le vérificateur général signale toutefois le besoin
de faire de nouveaux progrès dans les domaines du
contrôle et de la responsabilisation. À ce propos, il
fait allusion à l'établissement de mon poste et à
mon mandat, qu'il décrit comme un mécanisme
externe d'examen des activités de collecte de ren-
seignement étranger du CST.

Le vérificateur général exprime l'avis que les
activités de mon bureau devraient permettre au
Parlement d'examiner et de débattre le sujet de
manière plus éclairée, dont la question de savoir
s'il serait dans l'intérêt public d'envisager l'éta-
blissement d'un cadre législatif pour le CST. Il
conclut en exhortant le gouvernement à étudier
les avantages d'un tel cadre.

Mes premières tâches, après ma nomination, ont
consisté à établir mon bureau et à le doter en per-
sonnel. Grâce au concours de fonctionnaires du
Bureau du Conseil privé et du ministère de la
Défense nationale, on m'a bientôt installé un
bureau dans le centre-ville d'Ottawa. Toutefois, il a
fallu modifier les locaux afin de satisfaire aux
normes de manipulation et d'entreposage de docu-
ments classifiés. En septembre, mon bureau était
établi et totalement opérationnel.

Demandes d'examen et de responsa- bilité

des renseignements délicats véhiculés par les réseaux téléphoniques et informatiques de l'État, ainsi qu'à protéger l'intégrité et la disponibilité de l'information gouvernementale.

Ma nomination, en juin 1996, est survenue à un moment opportun pour diverses raisons. Premièrement, le mois suivant, le commissaire à la protection de la vie privée a publié un rapport adressé au chef du CST, dans lequel il exposait dans le détail les conclusions d'une vérification de conformité qu'il avait achevée peu de temps auparavant. Ce rapport est classifié, toutefois, le commissaire à la protection de la vie privée y a fait allusion dans son rapport annuel, qui est un document public. Il y a mentionné que, pour diverses raisons, dont l'absence de cadre législatif, la vérification faite au CST s'était avérée une tâche complexe. Il a signalé, en particulier, qu'« au cours de la vérification, [il y avait eu] diverses allégations publiques accusant le CST de recueillir des renseignements sur la population et les partis politiques canadiens ».

Le commissaire à la protection de la vie privée a passé en revue un échantillon représentatif de données et de rapports de renseignements électromagnétique et conclu que le CST recueille uniquement l'information qui répond aux critères établis par le gouvernement touchant le renseignement étranger. Il n'a trouvé aucune preuve susceptible de corroborer des allégations selon lesquelles le CST ciblerait des Canadiens ou surveillerait leurs communications. Le CST utilise des procédures rigoureuses pour réduire au minimum la possibilité de capter par inadvertance des renseignements concernant des Canadiens. Le commissaire à la protection de la vie privée a conclu que, dans la mesure où sa vérification lui permettait de l'établir, le CST exerce son activité en conformité avec la Loi sur la protection des renseignements personnels et

Etats-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande, et chacun de ces pays possède une organisation semblable au CST.

Mandat du CST

Le CST est aujourd'hui l'organisme cryptologique national du Canada. Dans l'exercice de son mandat touchant le renseignement électromagnétique, il recueille et analyse les transmissions électroniques faites par d'autres pays par radio, par radar ou par d'autres moyens; il reçoit à cette fin l'aide du Réseau radio supplémentaire des Forces canadiennes qui possède un certain nombre de stations un peu partout au pays.

Le CST contribue au programme gouvernemental de renseignement étranger par l'interception des transmissions électroniques. On entend par renseignement étranger l'ensemble de l'information ou des renseignements au sujet des moyens, des intentions ou des activités d'Etats étrangers, d'entreprises ou de personnes de ces pays recueillis dans le cadre de la défense du Canada ou de la conduite de ses affaires internationales. Cela peut comprendre de l'information de nature politique, économique, militaire, scientifique ou sociale susceptible d'avoir des incidences sur la sécurité.

Dans le cadre de son programme de STI, le CST fournit des avis, des conseils et des services techniques sur les moyens d'assurer la sécurité des télécommunications de l'Etat et sur divers aspects de la sécurité du traitement électronique de données. Son objectif consiste à aider le gouvernement fédéral à protéger convenablement la sécurité de ses télécommunications et de ses systèmes d'information automatisés. Il atteint cet objectif en fournissant aux ministères les moyens et les conseils voulus pour garantir la protection de leurs renseignements classifiés et désignés. Dans ce sens, le service fourni par le CST vise à empêcher toute personne ou organisation non autorisée d'accéder à

On a d'abord déterminé qu'il fallait continuer d'intercepter des transmissions électroniques pour protéger les intérêts du Canada à l'étranger et en matière de défense. La décision du gouvernement a été influencée par les demandes de maintien de l'aide à la collecte de renseignements faites par les États-Unis et la Grande-Bretagne, et par les révélations du transfuge soviétique Igor Gouzenko touchant les activités de renseignement menées par l'URSS au Canada et aux États-Unis. C'est ainsi qu'est né le mandat du CST touchant le renseignement électromagnétique.

Il était par ailleurs évident que les ministères et organismes du gouvernement fédéral avaient désormais besoin de conseils et d'aide pour protéger leurs renseignements classifiés contre l'interception par des parties hostiles. C'est ainsi qu'à vu le jour le mandat défensif du CST, appelé à l'époque sécurité des télécommunications (COMSEC) et maintenant sécurité des technologies de l'information (STI).

Cette nouvelle organisation cryptologique nationale en temps de paix, établie par décret en 1946 et rebaptisée Direction des communications du Conseil national de recherches, s'est vu confier la responsabilité du renseignement électromagnétique et de la sécurité des télécommunications. En 1975, elle a été transférée par décret au ministère de la Défense nationale, et le Ministre a assumé la charge d'activités désignées conformément à l'article 4 de la *Loi sur la défense nationale*. L'organisation a en même temps été rebaptisée Centre de la sécurité des télécommunications.

Par l'intermédiaire du CST, le Canada continue à entretenir des rapports de collaboration avec certains de ses proches alliés de longue date pour l'échange de renseignements étranger et le partage en matière de sécurité des technologies de l'information de nature délicate. Ces alliés sont les

À mesure que la guerre avançait et que le volume des données brutes augmentait, le besoin pour le Canada de disposer de ses propres moyens d'encodage et de décryptage faisait l'objet de discussions entre les représentants du gouvernement canadien, dont ceux de l'armée, du ministère des Affaires extérieures (MAE), de la Gendarmerie royale du Canada (GRC) et du Conseil national de recherches. Au cours de cette période de débat, les Américains et les Britanniques ont exprimé l'avis que le Canada devait devenir un participant actif et se doter de ses propres compétences dans ce domaine.

En 1941, à l'exhortation du ministère des Affaires extérieures, le gouvernement a établi un bureau national du renseignement électromagnétique appelé Sous-section de l'examen. Celle-ci était rattachée au Conseil national de recherches et comprenait des représentants de la GRC, du MAE et des trois services militaires. Sous la coordination de la Sous-section de l'examen, des données interceptées brutes et des messages décryptés étaient alors utilisés par des consommateurs canadiens de renseignements et retransmis aux services SIGINT alliés en Grande-Bretagne et aux États-Unis, ou relayés en sens inverse. Les messages interceptés provenaient d'Union soviétique, d'Allemagne, d'Italie, d'Amérique du Sud et d'Asie. À la fin de la guerre, la Sous-section de l'examen, rebaptisée *Joint Discrimination Unit*, fonctionnait pleinement à titre de service du renseignement électromagnétique.

En 1944, des délibérations ont été entreprises (principalement entre des représentants du MAE, de l'armée et de la marine) afin de déterminer le besoin et la structure d'une éventuelle organisation de l'après-guerre ainsi que le rôle qu'elle jouerait pour répondre aux besoins de renseignement du gouvernement de l'époque. Les deux programmes à l'origine du mandat actuel du CST ont commencé à prendre forme à ce moment-là.

Le 9 mai 1996, j'ai pris ma retraite comme juge de la Cour d'appel du Québec après plus de vingt-sept années d'exercice de la magistrature. En assumant mes fonctions de commissaire du CST, j'ai été confronté aux divers aspects de la communauté de la sécurité et du renseignement du Canada en général et du CST en particulier. À cet égard, les origines du CST méritent d'être signalées.

Le rôle joué par le CST dans la collecte de SIGINT remonte à plusieurs décennies. En 1925, sous la direction de la Marine royale britannique (l'Amirauté), la Marine royale canadienne a établi la première installation de radiogoniométrie haute fréquence du Canada à la base navale d'Esquimalt, dans l'île de Vancouver. Au cours des années qui ont suivi, une série d'autres installations ont été mises sur pied d'un bout à l'autre du Canada, et les interceptions par radiogoniométrie haute fréquence ont permis d'aider l'Amirauté à repérer les navires dans l'océan Pacifique; celle-ci disposait déjà de stations couvrant l'Atlantique.

L'aide apportée par le Canada à la Grande-Bretagne a pris de l'ampleur dans les années 20 et 30. À ce moment-là, les activités de SIGINT englobaient non seulement le repérage et la surveillance de transmissions étrangères par radiogoniométrie haute fréquence, mais aussi la surveillance des interceptions de signaux de T.S.F. faites par l'armée canadienne et par le Service de radiotélégraphie du ministère des Transports. Après le déclenchement de la Seconde Guerre mondiale, la Grande-Bretagne a demandé au Canada de continuer à assurer ces services de radiogoniométrie et d'interception de renseignements bruts; ceux-ci étaient utilisés, par exemple, par la Marine royale britannique et par le service de sécurité des communications radiophoniques de Grande-Bretagne.

Ma nomination et mon mandat

télécommunications (CST) contribue à ces travaux par l'exécution des programmes prévus dans son mandat, soit, comme on les appelle communément, le renseignement électromagnétique étranger (SIGINT) et la sécurité des technologies de l'information (STI).

Je pense cependant que les citoyens du Canada ont raison de s'attendre à ce que les organismes tenus d'exercer une bonne partie de leurs activités sous le sceau du secret le fassent en conformité avec les lois du Canada. Il m'incombe de leur donner cette assurance en ce qui concerne le CST.

Le 19 juin 1996, le ministre de la Défense nationale a annoncé ma nomination au poste de commissaire du Centre de la sécurité des télécommunications en vertu de la partie II de la *Loi sur les enquêtes*, pour un mandat de trois ans. J'exerce cette fonction à temps partiel, et mon mandat, établi par décret, est le suivant :

- examiner les activités du CST en vue de déterminer si elles sont conformes à la loi;
- informer le ministre de la Défense nationale et le procureur général du Canada de toute activité qui m'apparaît non conforme à la loi;
- ne pas examiner les questions pour lesquelles il existe d'autres recours prévus par des lois;
- présenter au Ministre des rapports contenant des renseignements classifiés lorsque je le juge à propos;
- présenter au Ministre un rapport annuel de mes activités et de mes constatations rédigé dans les deux langues officielles, pour dépôt au Parlement.

Le gouvernement du Canada s'appuie sur l'information et les renseignements obtenus par divers moyens et d'un grand nombre de sources pour protéger les biens et les intérêts du pays. La collecte, l'analyse et la diffusion de renseignements aident le Canada à s'acquitter de ses nombreuses obligations internationales, par exemple à l'égard du maintien de la paix et de la lutte contre le terrorisme.

Au cours des premiers mois qui ont suivi ma nomination, il m'est apparu que les personnes qui recueillent les renseignements comme celles qui les utilisent au Canada conviennent que la fin de la guerre froide a fait naître des défis nouveaux et complexes. En effet, l'information et les renseignements recueillis pendant les années 90 révèlent que les menaces planant sur la sécurité de nombreux pays, dont le Canada, se diversifient et augmentent. La volatilité et, dans certains cas, l'instabilité politiques, sociales et économiques, alliées à la disparition d'un ennemi commun, menacent les systèmes de défense et la sécurité à l'échelle mondiale.

La libre circulation des personnes et du matériel a accru la menace terroriste. Elle a en outre suscité des inquiétudes mondiales touchant la prolifération et la disponibilité des armes de destruction massive et contribué à l'expansion du crime organisé. La concurrence économique et technologique mondiale joue également un rôle dans cette évolution, et le nombre des cibles (personnes et organisations) possibles et connues a augmenté.

Face à ces défis, les organismes du gouvernement du Canada qui s'occupent de sécurité et de renseignement ont joué un rôle essentiel dans la collecte, l'analyse et la diffusion d'informations et de renseignements sur les questions touchant les intérêts nationaux. À titre de membre de la communauté canadienne de la sécurité et du renseignement, le Centre de la sécurité des

TABLE DES MATIÈRES

Avant-propos	1
Ma nomination et mon mandat	2
Origines du Centre de la sécurité des télécommunications (CST)	3
Mandat du CST	6
Demandes d'examen et de responsabilisation	7
Revue de la première année	8
• Activités	8
• Constatations	11
• Limites	13
Budget et personnel	13
Prochaines étapes	14
Annexe	15
• Décret C.P. 1996-899	15

Commissaire du Centre de la
sécurité des télécommunications



CANADA

L'honorable Claude Bisson

Communications Security
Establishment Commission

The Honourable Claude Bisson

Le 11 avril 1997

L'honorable Douglas Young
Ministre de la Défense nationale
et ministre des Anciens combattants
101, promenade du Colonel-By
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément à l'alinéa b) du décret C.P. 1996-899, prévoyant ma nomination au poste de commissaire du Centre de la sécurité des télécommunications, j'ai le plaisir de vous communiquer le premier rapport annuel de mes activités et constatations portant sur la période du 19 juin 1996 au 31 mars 1997, pour présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'expression de ma haute considération.

A handwritten signature in cursive script, reading "Claude Bisson".

L'honorable Claude Bisson

Bureau du Commissaire du Centre de la sécurité des télécommunications
C.P. 1984, Succursale «B»
Ottawa (Ontario)
K1P 5R5

Tél : (613) 992-3044
Télécopieur : (613) 992-4096

© Ministère des Travaux publics et des Services gouvernementaux Canada 1997
ISBN 0-662-62910-8
N° de cat. JS95-1997
ISSN 1206-7490



RAPPORT ANNUEL

du Commissaire du Centre de la sécurité
des télécommunications



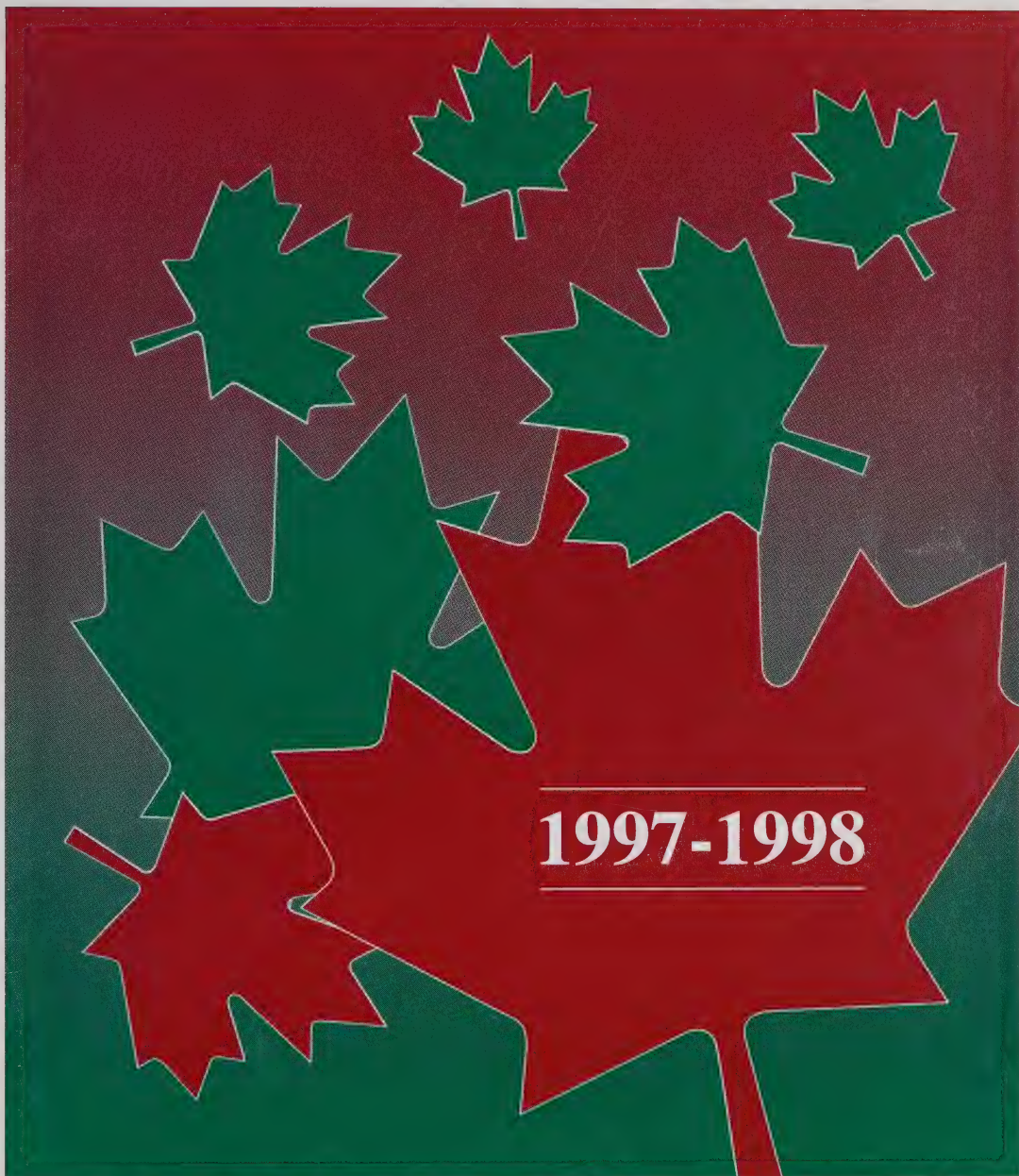
CAI
ND 800

-S16



ANNUAL REPORT

of the Communications Security
Establishment Commissioner



Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station 'B'
Ottawa, Ontario
K1P 5R5

Tel: (613) 992-3044
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 1998
ISBN 0-662-63603-1
Cat. No. D95-1998

Communications Security
Establishment Commissioner



The Honourable Claude Bisson

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Claude Bisson

May 1998

The Honourable Arthur C. Eggleton, P.C.
Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Mr. Eggleton:

Pursuant to paragraph (b) of Order in Council P.C. 1996-899 appointing me Communications Security Establishment Commissioner, I am pleased to submit to you my second annual report on my activities and findings from April 1, 1997 to March 31, 1998, for your submission to Parliament.

Yours sincerely,

The Honourable Claude Bisson



TABLE OF CONTENTS

The Year in Brief	1
Findings	1
• Foreign Intelligence Priorities	1
• SIGINT Policy at CSE	2
• Internal Investigations and Complaints	3
• Assertion on Lawfulness	4
The Review Network	5
Complaints	9
Reviewing CSE's Activities: A Permanent Model	10
• Legislation	11
• Reporting	11
• Mandate	11
• Legislation in Other Countries	11
Legislation for CSE	12
Budget and Staff	12
Appendix	15
• Order in Council P.C. 1996-899	15

The Year in Brief

This is my second Annual Report, and it covers the period ending March 31, 1998. It was a busy year that included extensive meetings and briefings with officials at the Communications Security Establishment (CSE) and other government departments, submitting periodic classified reports to the Minister of National Defence on my study findings, and forging new relationships and cementing old ones both in Canada and internationally.

I was ably represented at the first International Meeting of Inspectors General of Intelligence and Security in Canberra, Australia, in November and at follow-up discussions in Washington, D.C., in April 1998. I also had the pleasure of meeting and briefing members of the Parliamentary Intelligence and Security Committee of the United Kingdom in March 1998.

The capabilities of my Office were expanded during this period. I have a small professional staff and contractors with expertise in a variety of areas including high technology.

I discuss these topics in greater detail further on in this report, along with other matters that have captured my attention since my last report.

Findings

Foreign Intelligence Priorities

Each year, the Government establishes its intelligence requirements, including its foreign intelligence priorities. These priorities are then communicated in writing to the Chief of CSE, by the Security and Intelligence Coordinator, Privy Council Office. As part of its response, CSE develops a business plan that guides the signals intelligence (SIGINT) program.

I examined the foreign intelligence priorities and the SIGINT business plan and I am able to confirm that for the fiscal year 1997/98, CSE's activities were consistent with these priorities.

SIGINT Policy at CSE

In the course of my review activities, I had occasion to look at CSE's framework for SIGINT policies with lawfulness implications. I wanted to examine specific CSE policies to determine whether they provided adequate guidance to employees in the performance of their duties. I was particularly interested in policies related to privacy issues.

I found CSE's SIGINT policies to be sound. The policies in place, as well as the system under which they are developed, appear to be well conceived. Moreover, the procedural documentation drafted in support of these policies is comprehensive and clearly stated.

During my examination of these policies, I did observe that while CSE has an appreciable amount of policy, it is not always at the right organizational level. However, I did not encounter any major SIGINT policy gaps, and I can provide my assurance that none of the gaps related to the lawfulness of CSE's activities or to the privacy of Canadians.

I noted that a cornerstone of CSE's SIGINT policies deals with safeguarding the privacy of Canadians. It applies to information in the possession of CSE, for the purpose of providing the government with foreign signals intelligence, in support of its foreign and defence policies.

I was able to observe that the policies require CSE employees to conduct their operational activities in strict recognition of, and adherence to, federal legislation governing the protection of the rights, privacy and freedoms of Canadians. The policies affirm CSE's commitment to respect the corresponding procedures of its close and long-standing allies, Australia, New Zealand, the United Kingdom and the United States (also known as the Second Parties). However, these procedures must conform first to the laws of Canada.

CSE undertakes explicitly to treat the communications of Second Party nationals in a manner consistent with the procedures issued by the agency of that country, provided such procedures do not contravene the laws of Canada. This is a reciprocal undertaking to ensure that the Second Parties do not target each others' communications or circumvent their own legislation by targeting communications at each others' behest. In other words, they do not do indirectly what would be unlawful for them to do directly.

During discussions, CSE officials referred to their key SIGINT policies as "living, breathing documents." In this regard, I noted that these policies are the subject of ongoing internal review. I also found that the policy design includes indicators to measure the effectiveness of the policy, one of which is the result of any audit carried out by the Privacy Commissioner. (I referred to his most recent findings on this topic in my last report.) Historically, these indicators have been used to guide subsequent iterations of the policy.

Among the mechanisms used to ensure that employees acquire the knowledge they need to discharge their duties lawfully are training on policies and on-the-job mentoring. I learned that over the past year, employees were also brought together to participate in an exercise to identify, among other things, the organization's core values. CSE officials stated that, without exception, all focus groups of employees identified the value of lawfulness as a core CSE value.

Internal Investigations and Complaints

I was interested to learn about internal investigations and complaints at CSE. I examined reports and documents pertaining to all incidents involving employees since my appointment in June 1996. I wanted to know whether any of the incidents involved unlawful activity in the delivery

of CSE's mandate. To protect the privacy rights of the individuals involved, procedures were adopted to ensure that their names and any other identifiers were shielded from view.

The incidents I reviewed involved a variety of matters such as miscellaneous internal security violations and infractions; however, there were no discernible trends. None of the incidents involved unlawful activity in relation to CSE's mandate, or infringements on the privacy of Canadians.

I also wanted to know what procedures were in place for employees who resign or are released. I learned that CSE had identified, and is in the process of implementing, a comprehensive program to address these and other matters. This is a positive first step, and I intend to look at it again at a future date.

Assertion on Lawfulness

During the year under review, my office refined its procedures for examining the electronic gateway to the information collected and held by CSE. Based on the results of this review and analysis, I am of the opinion that CSE has acted lawfully in the performance of its mandated activities since my last report. I am also satisfied that CSE has not targeted Canadian citizens or permanent residents.

In giving assurance that CSE does not target the communications of Canadians, I would like to add, for greater certainty, that this applies to all Canadians, including the people of Québec. CSE does not target Québec communications, or the Québec sovereignty movement, and it does not have a "French Section".

The Order in Council appointing me CSE Commissioner appears in an appendix to this report. Paragraph (c) authorizes me to submit a report containing classified information to the

Minister of National Defence any time I consider it advisable. Since my last report, I have submitted three classified reports to the Minister. None of these reported on unlawful activity on the part of CSE.

The Review Network

The first International Meeting of Inspectors General of Intelligence and Security was held in Canberra, Australia, in November 1997. Office holders responsible for reviewing the activities of all or parts of the security and intelligence community of their respective countries were present from Australia, New Zealand, the United Kingdom, the United States, South Africa and Canada. The South African delegates were afforded a warm welcome given that their country's national institutions, particularly their security and intelligence agencies, are in transition following the end of apartheid.

The meeting was held at the initiative of the former Australian Inspector General, in honour of the tenth anniversary of his Office. It provided a welcome opportunity for participants to exchange information and ideas, to discuss trends and to compare models for effective review and oversight.

A broad array of options and alternatives was apparent in the mandates and organizational arrangements of the Inspectors General represented at the meeting. Some have legislated mandates, such as those in Australia, New Zealand and Canada's Inspector General of the Canadian Security Intelligence Service (CSIS). Others are independent of, or embedded in, the agencies they oversee. The mandates of Inspectors General in the United States run the gamut of these alternatives, and there do not appear to be hard and fast rules regarding the scope of their responsibilities or their degree of independence from the agency under their review.

It was also interesting to note the array of options for parliamentary review and oversight mechanisms. Representing the parliamentary review model were members of the United Kingdom's Parliamentary Intelligence and Security Committee, described as a committee of parliamentarians rather than a formal statutory committee of Parliament; Canada's Security Intelligence Review Committee, composed of three to five Privy Councillors appointed by the government to review the activities of CSIS; and members of the Joint Standing Committee on Intelligence, a committee of parliamentarians in South Africa where the government is in the process of identifying a model for intelligence oversight. In addition, participants met with Australia's Parliamentary Joint Committee on the Australian Security Intelligence Organization (ASIO) as part of the program.

While there were obvious commonalities, a wide range of mandated review or oversight activities was evident among the participants. These included such responsibilities as

- monitoring the lawfulness of the agency's activities,
- safeguarding the rights of citizens,
- investigating incidents and operational activities that generated public controversy,
- investigating complaints received from a variety of sources,
- investigating security practices, access to information and privacy concerns,
- monitoring activities and reporting findings to the legislative or the executive arm of government, and
- providing assurance to the responsible Minister or member of Cabinet.

Some participants had responsibilities as diverse as investigating fraud, waste and abuse of resources and uncovering criminal activity.

Each country's review and oversight mechanisms tend to be structured according to the division of roles, mandates and powers between their parliamentary and non-parliamentary bodies, or their executive and legislative branches of government. The division of these elements is influenced by a variety of factors, such as

- the presence or absence of enabling legislation for the agencies under review,
- the nation's preference for parliamentary versus non-parliamentary (or executive versus legislative) responsibility for review and oversight of security and intelligence agencies,
- the existence of other statutory bodies (in Canada, for example, the Information and Privacy Commissioners and the Auditor General).

It was clear that in each country represented, a determination had been made regarding the best means of achieving effective review or oversight, drawing from the pool of expertise represented by elected officials, parliamentary appointees and bureaucrats.

There was consensus that review and oversight had evolved over the years and would continue to evolve, particularly in those countries where enabling legislation has been enacted most recently. Of particular note was the general agreement that the very presence of review and oversight mechanisms tends to alter the dynamics of security and intelligence agencies, causing them to assess and, if necessary, modify the way they conduct business. Over time, these agencies have

begun to appreciate that there are benefits to review and oversight, including the capability to identify and resolve problems within their own walls.

Despite the differing review and oversight mandates of those present, a number of common issues and themes emerged. For example, increased demands for greater transparency and accountability in government were a common backdrop to the activities of all participants.

Independence and objectivity were identified as essential to successful review. Overall, relationships between the review or oversight bodies and their respective agencies were characterized as formal, proper and generally cordial. All participants agreed that maintaining independence and building confidence and credibility, not only with the agency being reviewed but with the public, is a constant and delicate balancing act. They also acknowledged the inherent difficulty of maintaining public confidence on those occasions when they find no fault in the activities of the bodies they oversee or review. There was consensus, however, that maintaining the right balance was facilitated by time and experience.

The Canberra meeting opened the door for further discussions during the year. In March, I had the opportunity to pursue some of these themes in further detail when the members of the United Kingdom's Parliamentary Intelligence and Security Committee visited Ottawa as part of their North American agenda of consultations. Subsequently, in April, my staff had fruitful discussions with some of my American counterparts in Washington, D.C.

To sum up, it was clear from these discussions that review and oversight mechanisms are relatively new features in the security and intelligence community worldwide, and that they continue to evolve. They play an important role in responding to calls for greater transparency and accountability

in government. By their very presence, these mechanisms encourage security and intelligence agencies to assess and, if necessary, modify the way they conduct business.

I am of the opinion that our small community of independent monitors can continue to reap significant benefits by sharing their collective wisdom on these topics.

Complaints

As I explained in my last report, I am precluded from reviewing CSE-related matters for which other avenues of redress are established by statute. Moreover, my review is confined to those issues that relate to CSE's mandate. Furthermore, and as I stated at the time of my appointment, I will not review incidents that occurred before my appointment.

I also referred, in my last report, to a limitation in my mandate regarding complaints. While I can review allegations about certain of CSE's activities, I am unable to follow up with individual complainants to tell them about my examination of their allegations and my findings.

This situation remains unchanged today. As a result, I must once again ask those concerned to derive some comfort from the general assurances I have provided elsewhere in this report on the lawfulness of CSE's activities.

It is clear that this is not a satisfactory situation. Individuals who are concerned about the activities of an agency of government ought to have recourse to an independent office where their complaints can be heard and examined.

I am optimistic, however, that this matter will be resolved in the near future, and hopefully before my next report.

Reviewing CSE Activities: A Permanent Model

As I approach my third year as Commissioner I am frequently asked what will happen to my Office at the end of my mandate in June 1999. While this decision ultimately rests with the Government, I anticipate that a number of opinions will be voiced by a variety of interested parties, along with ideas on the best model for a permanent review mechanism.

Over the past two years, I have had many opportunities to reflect on this subject, and to consider a possible structure. As my starting point, I looked at my own Office and the attributes and requirements that I identified to discharge my current mandate. Among them are

- independence,
- clearly defined mandate and reporting,
- knowledge and understanding of CSE's operational methods and activities,
- understanding of the laws of Canada and their application,
- effective means of assessing the lawfulness of CSE's activities,
- a professional relationship with CSE's officials,
- effective relationships with other interested parties in government, and
- adequate and appropriate resources.

I have also identified four elements that could have an impact on the model selected, even if they go beyond the immediate requirements and structure of a review mechanism.

Legislation

While it is clear that enabling legislation is not required to establish a permanent review mechanism for CSE, the review mechanism itself ought to be incorporated eventually in a constituent act. This raises a number of policy and related questions for the drafters of the legislation, as is evident from the array of options represented at the meeting in Australia.

Reporting

Under the provisions of my Order in Council, I submit my reports to the Minister of National Defence. Based on my experience to date, I am of the opinion that this arrangement works well. However, I have also observed that some of my counterparts, both in Canada and abroad, report directly to Parliament. This alternative should also be examined for the permanent review mechanism.

Mandate

My mandate is set out in the Order in Council, reproduced in an appendix to this report. It was evident from my discussions with colleagues that I have a very focused mandate. While I believe it is adequate under the present circumstances, consideration should be given to exploring alternatives for the mandate of a permanent review mechanism. It is important to ensure any permanent mechanism gives the Government, and the public, an appropriate degree of comfort with respect to CSE's activities.

Legislation in Other Countries

I found great value in the exchange of ideas and experiences with my colleagues in other countries. A review of their legislation and further consultations might be of benefit. While I believe that this might reveal the need for a uniquely Canadian solution, there is often much to be learned from other countries, particularly the parliamentary models of the United Kingdom, Australia and New Zealand.

Legislation for CSE

In my last report, I indicated that there was support in a number of circles for enabling legislation for CSE, and this continues to be the case. I also identified several policy issues that I thought should be studied or revisited prior to drafting, including the scope and structure of a legislative framework, control and accountability issues, and the scope and structure of enshrined review mechanisms.

During the past year, I have observed a great deal of hard work to grapple with fundamental issues affecting CSE and its place in government. Moreover, I have noted increased efforts toward greater openness on matters related to CSE. I applaud these initiatives because they help build public confidence in an agency that makes an important, if secret, contribution to the government's priorities and to Canada's security and defence interests.

Drafting legislation for CSE will be a challenge that should not be underestimated, in view of the rapid pace of change in the worlds of security and intelligence and technology. I anticipate animated debates on the topic.

Budget and Staff

My annual budget allocation remained unchanged at \$500,000 for the 1997/98 fiscal year. I am able to report that during my office's second year of operation, I discharged my mandated activities within budget.

I have a full-time working staff of two as well as a complement of people on contract who bring many years of experience in a variety of fields related to the work of my office. Some of my staff are well versed in the workings of Canada's security and intelligence community; others have special expertise in research, policy development, writing, editing and communications. More recently, I have engaged an adviser on high technology.

The year 1997/98 was my Office's first full year of operations, and it was filled with challenges and opportunities. I am satisfied with the structure and operation of my Office, and I believe that I have both the resources I need and the access to CSE that I require to discharge my responsibilities in the year ahead.



CANADA

PRIVY COUNCIL • CONSEIL PRIVÉ

P.C. 1996-899
June 19, 1996

His Excellency the Governor General in Council, on the recommendation of the Minister of National Defence, pursuant to Part II of the *Inquiries Act*, hereby authorizes the Minister of National Defence ("Minister"):

- (a) to appoint the Honourable Claude Bisson of Montreal, Quebec, for a period of three years, as a commissioner ("Commissioner") to review the activities of the Communications Security Establishment ("CSE") for the purpose of determining whether those activities are in compliance with the law;
- (b) to direct the Commissioner to submit to the Minister, once each year and in both official languages, a report on the Commissioner's activities and findings that are not of a classified nature, which report the Minister will table in Parliament;
- (c) to authorize the Commissioner, at any time the Commissioner considers it advisable, to submit a report containing classified information to the Minister;
- (d) to direct the Commissioner to advise the Minister and the Attorney General of Canada of any activity of CSE that the Commissioner believes may not be in compliance with the law;
- (e) to direct the Commissioner not to review issues for which other avenues of redress are established by statute;

.../2

- 2 -

(f) to require that the Commissioner and all persons engaged on his behalf take an oath of secrecy and comply with all applicable government security requirements;

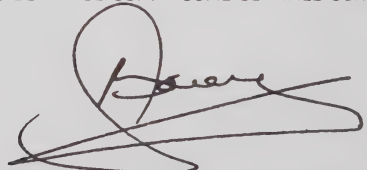
(g) to direct the Commissioner, before submission of any report to the Minister, to consult with the Deputy Clerk, Security and Intelligence, and Counsel at the Privy Council Office for the purpose of ensuring compliance with all security requirements and preservation of the secrecy of sources of security and intelligence information and of the security of information provided to Canada in confidence by other nations;

(h) to authorize the Commissioner to engage the services of such staff and technical advisors as he considers necessary to assist him in his review, at such rates of remuneration and reimbursement as may be approved by the Treasury Board;

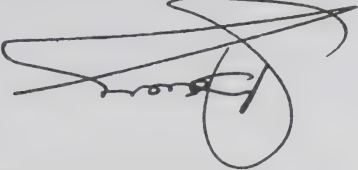
(i) to fix the remuneration of the Commissioner at the per diem rate set out in the schedule hereto, which rate is within the range of \$400 to \$500; and

(j) to authorize that the Commissioner be reimbursed for his actual transportation expenses and a non-accountable living allowance of up to \$175 per diem while in travel status away from his normal place of residence in connection with the conduct of this review.

CERTIFIED TO BE A TRUE COPY - COPIE CERTIFIÉE CONFORME



CLERK OF THE PRIVY COUNCIL - LE GREFFIER DU CONSEIL PRIVÉ



CERTIFIED TO BE A TRUE COPY - COPIE CERTIFIÉE CONFORME

I) à fixer la rémunération du commissaire au taux journalier établi dans l'annexe ci-jointe, lequel taux se situe dans l'échelle de 400 \$ à 500 \$; j) à autoriser le remboursement des frais de transports réels du commissaire ainsi qu'une allocation de subsistance non à justifier allant jusqu'à 175 \$ par jour lors de son déplacement à l'extérieur de son lieu de résidence habituel dans l'exercice des fonctions de cette enquête.

h) à autoriser le commissaire à retenir les services des experts et du personnel qu'il juge nécessaires pour l'assister dans son enquête, aux taux de rémunération que peut approuver le Conseil du Trésor;

g) à ordonner au commissaire, avant la présentation de tout rapport au ministre, de consulter le sous-greffier, sécurité et renseignement et conseiller juridique au Bureau du Conseil privé en vue de veiller à ce que toutes les exigences visant la sécurité soient respectées et que la confidentialité des sources de sécurité et de renseignements secrets et la sécurité de l'information fournie au Canada par d'autres nations à titre confidentiel soit protégée;

f) à exiger que le commissaire et toutes les personnes engagées pour son compte prononcent un serment de discrétion et se conforment à toutes les exigences du gouvernement applicables au secret;



Sur recommandation du ministre de la Défense nationale et en vertu de la partie II de la Loi sur les enquêtes, Son Excellence le Gouverneur général en conseil autorise le ministre de la Défense nationale (ci-après appelé le « ministre ») :

a) à nommer l'honorable Claude Bissson, de Montréal (Québec), pour une période de trois ans, commissaire pour faire enquête sur les activités du Centre de la sécurité des télécommunications (* CST *) en vue de déterminer si ces activités sont conformes à la loi;

b) à ordonner au commissaire de présenter au ministre, une fois l'an et dans les deux langues officielles, un rapport sur ses activités et ses constatations qui ne sont pas de nature classifiée, lequel rapport sera déposé par le ministre auprès du Parlement;

c) à autoriser le commissaire à soumettre au ministre tout rapport classifié, aux moments où il le juge indiqué;

d) à ordonner au commissaire d'aviser le ministre et le procureur général du Canada au sujet de toute activité du CST qu'il estime ne pas être conforme à la loi;

e) à ordonner au commissaire de ne pas examiner les questions pour lesquelles il existe d'autres recours statutaires;

Certains membres de mon personnel sont bien au courant des rouages de la communauté canadienne de la sécurité et du renseignement; d'autres ont des compétences particulières en recherche, en élaboration de politiques, en rédaction, en révision et en communications. Dernièrement, j'ai embauché un conseiller en technologie de pointe.

1997-1998 a été la première année d'activité complète de mon bureau, et elle a été riche en défis et en possibilités. Je suis satisfait de la structure et du fonctionnement de mon bureau, et j'estime avoir à la fois les ressources qu'il me faut et l'accès au CST dont j'aurai besoin pour m'acquitter de mes responsabilités au cours de l'année à venir.

J'ai signalé dans mon dernier rapport qu'un certain nombre de groupes appuyaient l'instauration d'une loi devant régir le CST, et il en est toujours ainsi. J'ai en outre recensé plusieurs questions de principe qui, à mon avis, devraient être étudiées ou réexaminées avant qu'on ne rédige cette loi, notamment la portée et la structure du cadre législatif, les questions de contrôle et de responsabilisation, ainsi que la portée et la structure des mécanismes d'examen qui seront prévus dans la loi.

Au cours de l'année écoulée, j'ai vu se faire beaucoup de travail ardu pour aborder les questions fondamentales intéressant le CST et sa place au sein du gouvernement. J'ai en outre remarqué les efforts accrus déployés pour faire preuve d'une plus grande ouverture sur les questions se rapportant au CST. J'applaudis à ces initiatives, car elles aident à susciter la confiance du public envers un organisme qui apporte une contribution importante, quoique secrète, aux priorités du gouvernement et aux intérêts du Canada en matière de sécurité et de défense.

La rédaction d'une loi devant régir le CST constituera un défi qu'il ne faut pas sous-estimer, compte tenu de l'évolution rapide de l'univers de la sécurité et du renseignement et de la technologie. Je m'attends à des débats animés sur cette question.

Le budget annuel qui m'a été alloué est resté le même, soit 500 000 \$ pour l'année financière 1997-1998. Je suis à même de signaler qu'au cours de ma deuxième année d'activité, je me suis acquitté de mon mandat dans les limites de ce budget.

Je dispose de deux employés à plein temps ainsi que d'un effectif de personnes engagées par contrat qui possèdent de nombreuses années d'expérience dans divers domaines liés au travail de mon bureau.

La loi

Il est clair qu'une loi habilitante n'est pas requise pour établir un mécanisme permanent d'examen des activités du CST, mais ce mécanisme lui-même devrait être intégré, avec le temps, dans une loi constitutive. Cela soulève un certain nombre de questions de principe et autres pour les rédacteurs de la loi, comme en témoigne la gamme des possibilités représentées à la réunion tenue en Australie.

La filière hiérarchique

Selon les dispositions du décret instituant ma charge, je présente mes rapports au ministre de la Défense nationale. En me fondant sur mon expérience des deux dernières années, je suis d'avis que cet arrangement fonctionne bien. Toutefois, j'ai par ailleurs observé que certains de mes homologues, tant au Canada qu'à l'étranger, font rapport directement au Parlement. On devrait également examiner cette solution de rechange pour le mécanisme d'examen permanent.

Le mandat

Mon mandat est énoncé dans le décret qui est reproduit en annexe. Mes entretiens avec des collègues ont clairement révélé que ce mandat est très circonscrit. J'estime qu'il est suffisant dans les circonstances actuelles, mais il y aurait lieu d'envisager d'autres possibilités pour le mandat d'un mécanisme d'examen permanent. Il importe d'assurer que celui-ci donnera au gouvernement, de même qu'au public, un degré de tranquillité d'esprit approprié quant aux activités du CST.

Lois dans les autres pays

J'ai trouvé très utile d'échanger des idées et des expériences avec mes collègues d'autres pays. On pourrait retirer des avantages d'un examen de leurs lois et d'autres consultations. Je pense que ces démarches révéleront peut-être le besoin d'une formule typiquement canadienne, mais on peut souvent tirer nombre d'enseignements des autres pays et, en particulier, des modèles parlementaires du Royaume-Uni, de l'Australie et de la Nouvelle-Zélande.

Modèle permanent d'examen des activités du CST

À la veille de ma troisième année au poste de commissaire, on me demande souvent ce qu'il adviendra de ma charge à la fin de mon mandat, en juin 1999. Cette décision relève en définitive du gouvernement, mais je prévois que diverses parties intéressées exprimeront un certain nombre d'opinions ainsi que des idées quant au meilleur modèle de mécanisme d'examen permanent.

Au cours des deux dernières années, j'ai eu nombre d'occasions de réfléchir à cette question et d'envisager une structure possible. J'ai pris comme point de départ ma propre charge et les traits et exigences que j'ai recensés pour m'acquitter de mon mandat actuel, notamment :

- l'indépendance;
- un mandat et une filière hiérarchique clairement définis;
- la connaissance et la compréhension des méthodes de fonctionnement et des activités du CST;
- la compréhension des lois du Canada et de leur application;
- des moyens efficaces d'évaluer la légalité des activités du CST;
- des relations professionnelles avec les responsables du CST;
- des rapports efficaces avec d'autres parties intéressées du gouvernement;
- des ressources suffisantes et adéquates.

J'ai en outre recensé quatre éléments qui pourraient influencer sur le modèle choisi, même s'ils vont au delà des exigences immédiates et de la structure d'un mécanisme d'examen.

Plaintes

Je suis d'avis que notre petit groupe de surveillants indépendants peut continuer à retirer des avantages importants de l'échange de connaissances avec leurs homologues sur ces sujets.

Comme je le mentionnais dans mon dernier rapport, je suis dans l'impossibilité d'examiner les questions intéressant le CST pour lesquelles il existe d'autres recours prévus par la loi. De plus, mon travail d'examen se limite aux questions se rapportant au mandat du CST. Par ailleurs, comme je l'ai déclaré lors de ma nomination, je n'examinerai pas les incidents survenus antérieurement.

J'ai également fait allusion, dans mon dernier rapport, à la limitation de mon mandat touchant les plaintes. Je peux en effet examiner les allégations relatives à certaines activités du CST, mais il m'est impossible d'assurer un suivi auprès des plaignants pour les informer de l'exécution de mon examen et de mes constatations.

Cette situation reste inchangée. En conséquence, je dois inviter de nouveau les personnes concernées à tirer un certain réconfort des assurances générales que je donne ailleurs dans le présent rapport au sujet de la légalité des activités du CST.

Ce n'est manifestement pas la une situation satisfaisante. Les personnes qui s'inquiètent des activités d'un organisme gouvernemental devraient avoir accès à un bureau indépendant où leurs plaintes pourraient être entendues et étudiées.

J'ai cependant bon espoir de voir cette question résolue dans un proche avenir et, avec un peu de chance, avant mon prochain rapport.

L'indépendance et l'objectivité ont été désignées comme essentielles au succès du travail d'examen. Dans l'ensemble, les relations entre les organismes d'examen ou de surveillance et les organismes surveillés ont été décrites comme conformes aux règles, correctes et généralement cordiales. Tous les participants ont convenu qu'ils sont constamment sur la corde raide en raison du besoin de maintenir leur indépendance et de gagner la confiance non seulement de l'organisme surveillé mais aussi du public. Ils ont en outre reconnu la difficulté qu'ils doivent surmonter pour garder la confiance du public dans les cas où ils ne trouvent rien à redire aux activités des organismes soumis à leur surveillance ou à leur examen. Ils ont cependant convenu de façon générale que le temps et l'expérience aident à atteindre un juste équilibre en la matière.

La réunion de Canberra a ouvert la voie à d'autres discussions au cours de l'année. Ainsi, en mars, j'ai eu l'occasion d'examiner plus à fond certains de ces thèmes lorsque les membres du comité parlementaire du renseignement et de la sécurité du Royaume-Uni sont venus à Ottawa dans le cadre de leur programme de consultations en Amérique du Nord. En avril, mon personnel a eu des entretiens fructueux avec certains de mes homologues américains à Washington (D.C.).

En résumé, il est ressorti de ces entretiens que les mécanismes d'examen et de surveillance sont des éléments relativement nouveaux de la communauté de la sécurité et du renseignement partout dans le monde, et qu'ils continuent d'évoluer. Ils jouent un rôle important pour répondre aux demandes visant une transparence et une responsabilité accrues des gouvernements. Leur existence même encourage les organismes de sécurité et de renseignement à évaluer et, au besoin, à modifier leur façon de faire les choses.

- la présence ou l'absence d'une loi habilitante visant les organismes faisant l'objet de l'examen;
- le choix du pays de confier la responsabilité d'examiner et de surveiller les organismes de sécurité et de renseignement à un organisme parlementaire plutôt que non parlementaire (ou à l'organe exécutif plutôt que législatif);
- l'existence d'autres organismes établis par des lois (au Canada, par exemple, les commissaires à l'information et à la vie privée et le vérificateur général).

Il était manifeste que, dans chaque pays représenté, on avait décidé du meilleur moyen à prendre pour assurer un examen ou une surveillance efficace en puisant dans l'ensemble des compétences constituées par les élus, les personnes nommées par le Parlement et les fonctionnaires.

De façon générale, les participants ont été d'accord pour dire que l'examen et la surveillance avaient évolué au cours des années et continueraient de changer, en particulier dans les pays qui n'ont adopté une loi habilitante que tout dernièrement. Fait à noter, ils ont convenu que l'existence même de mécanismes d'examen et de surveillance tend à transformer la dynamique des organismes de sécurité et de renseignement, et les amène à évaluer et, au besoin, à modifier leur façon de faire les choses. Avec le temps, ces organismes ont commencé à se rendre compte des avantages inhérents à l'examen et à la surveillance, notamment la capacité de détecter des problèmes internes et d'y remédier.

Malgré la différence des mandats d'examen et de surveillance des participants, un certain nombre de questions et de thèmes communs se sont dégagés. Par exemple, les demandes croissantes visant une transparence et une responsabilisation accrues des gouvernements sont une toile de fond commune aux activités de tous les participants.

rencontre le comité mixte parlementaire sur l'organisme de renseignement de sécurité de l'Australie (ASIO) dans le cadre du programme de la réunion.

Tout en comportant des points communs manifestes, les fonctions d'examen ou de surveillance confiées aux participants présentaient une grande variété. Elles comprenaient des responsabilités comme les suivantes :

- surveiller la légalité des activités de l'organisme;
- protéger les droits des citoyens;
- faire enquête sur les incidents et les activités opérationnelles controversés par le public;
- faire enquête sur les plaintes en provenance de diverses sources;
- faire enquête sur les questions de pratiques en matière de sécurité, d'accès à l'information et de protection de la vie privée;
- surveiller les activités et faire rapport de leurs constatations à l'organe législatif ou exécutif du gouvernement;
- rassurer le ministre ou le membre du Cabinet responsable.

Certains participants avaient des responsabilités aussi diverses que faire enquête sur l'escroquerie, le gaspillage et l'abus des ressources et découvrir des activités criminelles.

Les mécanismes d'examen et de surveillance tendent à être structurés en fonction de la répartition des rôles, des mandats et des pouvoirs entre les organismes parlementaires et non parlementaires, ou entre les organes exécutif et législatif de chaque pays. Cette répartition est influencée par divers facteurs, comme :

Cette réunion avait été convoquée par l'ancien inspecteur général de l'Australie pour souligner le dixième anniversaire de l'institution de sa charge. Les participants ont salué l'occasion qu'elle leur a fournie d'échanger des renseignements et des idées, de discuter des tendances et de comparer des modèles d'examen et de surveillance efficaces. Les mandats et les formules d'organisation des bureaux des inspecteurs généraux représentés à la réunion se sont révélés extrêmement variés. Certains, comme ceux de l'Australie et de la Nouvelle-Zélande et l'inspecteur général du Service canadien du renseignement de sécurité (SCRS), ont un mandat prévu par la loi. D'autres sont indépendants des organismes qu'ils surveillent ou, au contraire, en font partie. Aux États-Unis, les mandats des inspecteurs généraux passent par toute la gamme de ces possibilités, et il ne semble pas exister de règles absolues touchant l'étendue de leurs responsabilités ni le degré de leur indépendance par rapport à l'organisme dont ils examinent les activités.

L'éventail des mécanismes d'examen et de surveillance parlementaires possibles s'est également révélé intéressant. Parmi les représentants du modèle d'examen parlementaire figuraient des membres du comité parlementaire du renseignement et de la sécurité du Royaume-Uni, désigné comme un comité de parlementaires plutôt que comme un comité réglementaire officiel du Parlement; le Comité de surveillance des activités du renseignement de sécurité du Canada, qui se compose de trois à cinq membres du Conseil privé nommés par le gouvernement pour passer en revue les activités du SCRS; et des membres du comité mixte permanent du renseignement, qui réunit des parlementaires d'Afrique du Sud, où le gouvernement est en train de définir un modèle en vue de la surveillance des activités de renseignement. Les participants ont en outre

Au cours de l'année sur laquelle a porté le présent examen, mon bureau a amélioré ses méthodes lui permettant d'étudier la passerelle électronique donnant accès aux renseignements recueillis et détenus par le CST. En me fondant sur les résultats de cet examen et de cette analyse, j'estime que, depuis mon dernier rapport, le CST a agi d'une manière légale dans l'exercice des activités faisant l'objet de son mandat. Je suis en outre convaincu qu'il n'a pas ciblé de citoyens ni de résidents permanents du Canada.

À ce propos, j'aimerais ajouter, pour plus de certitude, que le CST ne cible les communications d'aucun Canadien, résidents du Québec compris. Le CST ne cible pas de communications au Québec, non plus que le mouvement souverainiste québécois, et il n'a pas de « section française ».

Le décret en vertu duquel j'ai été nommé commissaire du CST est reproduit en annexe. L'alinéa c) m'autorise à présenter des rapports renfermant des renseignements classifiés au ministre de la Défense nationale lorsque je le juge à propos. Depuis mon dernier rapport, j'ai présenté trois de ces rapports classifiés au Ministre. Aucun n'avait trait à des activités illégales de la part du CST.

La première réunion internationale des inspecteurs généraux des activités de renseignement et de sécurité a été tenue à Canberrra (Australie), en novembre 1997. Les responsables de l'examen des activités de la totalité ou de certaines parties de la communauté de la sécurité et du renseignement de l'Australie, de la Nouvelle-Zélande, du Royaume-Uni, des États-Unis, de l'Afrique du Sud et du Canada y étaient présents. Les délégués sud-africains ont été chaleureusement accueillis compte tenu du fait que les institutions nationales de leur pays, en particulier les organismes de sécurité et de renseignement, sont en transition par suite de la fin de l'apartheid.

Enquêtes internes et plaintes

La formation relative aux politiques et le mentorat en cours d'emploi sont au nombre des moyens utilisés pour faire en sorte que les employés acquièrent les connaissances dont ils ont besoin pour s'acquitter de leurs fonctions en conformité avec la loi. J'ai appris qu'au cours de la dernière année, on avait en outre réuni les employés pour les faire participer à un travail de réflexion destiné à déterminer, entre autres, les valeurs fondamentales de l'organisation. Les responsables du CST ont déclaré que tous les groupes de discussion sans exception avaient désigné la légalité comme l'une de ces valeurs fondamentales.

Je souhaitais me renseigner sur les enquêtes internes et les plaintes au CST. J'ai donc examiné les rapports et les documents relatifs à tous les incidents touchant des employés, survenus depuis ma nomination, en juin 1996. Je voulais savoir si l'un ou l'autre de ces incidents avait eu trait à des activités illégales auxquelles on se serait livré dans l'exécution du mandat du CST. Afin de protéger les droits à la vie privée des personnes concernées, des mesures ont été prises pour camoufler leurs noms et tout autre détail pouvant permettre de les identifier.

Les incidents que j'ai passés en revue avaient trait à un certain nombre d'affaires telles que violations et infractions diverses à la sécurité interne; on ne relevait toutefois aucune tendance perceptible. Aucun des incidents n'avait trait à des activités illégales liées au mandat du CST, ni à des atteintes à la vie privée des Canadiens.

Je voulais en outre savoir quelles étaient les procédures en place pour les employés démissionnaires ou licenciés. J'ai appris que le CST avait établi un programme complet pour faire face à ces questions et à d'autres préoccupations, et qu'il est en train de le mettre en œuvre. Il s'agit là d'une première démarche constructive, et je me propose de l'examiner de nouveau ultérieurement.

J'ai été à même d'observer que les politiques obligent les employés du CST à effectuer leurs activités opérationnelles en tenant rigoureusement compte des lois fédérales régissant la protection des droits, de la vie privée et des libertés des Canadiens, et en s'y conformant strictement. Elles affirment l'engagement du CST à respecter les procédures correspondantes de ses proches alliés de longue date, soit l'Australie, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis (également appelés les Secondes Parties). Toutefois, ces procédures doivent d'abord être conformes aux lois du Canada.

Le CST s'engage explicitement à traiter les communications de ressortissants d'une Seconde Partie d'une manière compatible avec les procédures établies par l'organisme du pays concerné, à condition que celles-ci ne contreviennent pas aux lois du Canada. Il s'agit là d'un engagement réciproque destiné à assurer que les Secondes Parties ne ciblent pas leurs communications mutuelles ni ne contournent leurs propres lois en ciblant des communications sur l'ordre les unes des autres. Autrement dit, elles ne font pas indirectement des choses qui seraient illégales si elles les faisaient directement.

Lors d'entretiens, les responsables du CST ont qualifié leurs politiques fondamentales en matière de SIGNET de « documents vivants ». J'ai remarqué à cet égard que celles-ci font l'objet d'examens internes réguliers. J'ai également constaté que les politiques comportent des indicateurs destinés à mesurer leur efficacité; l'un de ceux-ci est le résultat de toute vérification effectuée par le commissaire à la protection de la vie privée. (J'ai fait allusion à ses constatations les plus récentes à ce sujet dans mon dernier rapport.) Ces indicateurs ont toujours servi à guider la rédaction des versions subséquentes de la politique.

Politique du CST en matière de SIGINT

J'ai examiné les priorités en matière de renseignement étranger et le plan d'activités relatif à SIGINT, et je suis en mesure d'affirmer que, au cours de l'année financière 1997-1998, les activités du CST ont concordé avec ces priorités.

Au cours de mes activités d'examen, j'ai eu l'occasion d'étudier le cadre des politiques du CST en matière de SIGINT qui ont des incidences sur le plan de la légalité. Je voulais examiner les politiques particulières de l'organisme afin de déterminer si elles procuraient des conseils suffisants aux employés pour leur permettre d'exercer leurs fonctions. Je me suis particulièrement intéressé aux politiques relatives aux questions de protection de la vie privée.

J'ai trouvé que les politiques du CST en matière de SIGINT étaient sensées. Celles-ci, de même que le système présidant à leur élaboration, semblent bien conçues. En outre, les documents de procédure établis à l'appui de ces politiques sont complets et clairement rédigés.

Lors de cet examen, j'ai constaté que le CST dispose d'une quantité appréciable de politiques, mais qu'elles ne se trouvent pas toujours au bon palier de l'organisation. Toutefois, je n'ai relevé aucune lacune importante en ce qui touche la politique en matière de SIGINT, et je peux garantir qu'aucune des lacunes n'avait trait à la légalité des activités du CST ni à la protection de la vie privée des Canadiens.

J'ai constaté que la protection de la vie privée des Canadiens constitue l'une des pierres angulaires de la politique du CST relativement à SIGINT. Celle-ci a trait aux renseignements que possède le CST afin de fournir au gouvernement des renseignements électromagnétiques étrangers à l'appui de ses politiques étrangères et de défense.

Ce rapport annuel, qui est mon deuxième, porte sur la période qui s'est terminée le 31 mars 1998. Il s'est agi d'une année bien remplie, au cours de laquelle j'ai tenu nombre de réunions et séances d'information avec des fonctionnaires du Centre de la sécurité des télécommunications (CST) et d'autres ministères, présenté des rapports périodiques classifiés au ministre de la Défense nationale sur mes constatations, établi des relations nouvelles et consolidé celles que j'avais déjà nouées tant au Canada que sur la scène internationale.

J'ai été représenté de façon très compétente à la première réunion internationale des inspecteurs généraux des activités de renseignement et de sécurité, tenue à Canberra (Australie), en novembre, ainsi qu'aux entretiens de suivi qui ont eu lieu à Washington (D.C.), en avril 1998. J'ai en outre eu le plaisir de rencontrer les membres du comité parlementaire du renseignement et de la sécurité du Royaume-Uni à l'occasion d'une séance d'information, en mars 1998.

Les moyens de mon bureau ont été renforcés au cours de cette période. Je dispose d'un petit groupe d'employés professionnels et d'entrepreneurs versés dans divers domaines, dont la technologie de pointe. Je développe ces sujets plus loin dans le présent rapport, de même que d'autres questions qui ont retenu mon attention depuis la rédaction de mon dernier rapport.

Chaque année, le gouvernement établit ses besoins en matière de renseignement, y compris ses priorités en matière de renseignement étranger. Celles-ci sont ensuite communiquées par écrit au chef du CST par le coordonnateur de la sécurité et du renseignement du Bureau du Conseil privé. Le CST établit, dans le cadre de sa réponse, un plan d'activités qui guide le programme de renseignement électromagnétique étranger (SIGINT).

TABLE DES MATIÈRES

L'année en bref	1
Constatations	1
• Priorités en matière de renseignement étranger	1
• Politique du CST en matière de SIGINT	2
• Enquêtes internes et plaintes	4
• Affirmation de la légalité	5
Le réseau des responsables de l'examen	5
Plaintes	10
Modèle permanent d'examen des activités du CST	11
• La loi	12
• La filière hiérarchique	12
• Le mandat	12
• Lois dans les autres pays	12
Loi devant régir le CST	13
Budget et personnel	13
Annexe	15
• Décret C.P. 1996-899	15

1997-1998

RAPPORT ANNUEL
du Commissaire du Centre de la sécurité
des télécommunications



CA1
ND 800
- S16

Publication
Publi



ANNUAL REPORT

of the Communications Security
Establishment Commissioner

1998-1999

Canada

Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station 'B'
Ottawa, Ontario
K1P 5R5

Tel: (613) 992-3044
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 1999
ISSN 1206-7490
Cat. No. D95-1999

Communications Security
Establishment Commissioner



Commissaire du Centre de la
sécurité des télécommunications

The Honourable Claude Bisson, O.C.

L'honorable Claude Bisson, O.C.

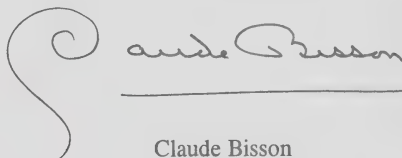
July 1999

The Honourable Arthur C. Eggleton, P.C.
Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Mr. Eggleton:

Pursuant to paragraph (b) of Order in Council P.C. 1996-899 appointing me Communications Security Establishment Commissioner, I am pleased to submit to you my third annual report on my activities and findings during the last year of my mandate, for your submission to Parliament.

Yours sincerely,



Claude Bisson



TABLE OF CONTENTS

Three Years of Reviewing CSE	1
• Looking Back on the First Mandate.....	2
• Technology, Privacy and Review.....	4
• The Effect of Review on CSE	5
1998-99 Activities	5
• Testing	6
• The Complaints Function	7
• Other Activities	9
• Budget and Staff.....	10
1998-99 Findings.....	10
Operational Policy Revisited.....	11
The Review Function	12
Farewell	13
Annex A: Order in Council P.C. 1996-899.....	15
Annex B: Statement of Expenditures	17

Three Years of Reviewing CSE

On June 19, 1996, the Minister of National Defence appointed me to the position of Communications Security Establishment (CSE) Commissioner for a period of three years, with the mandate to review the activities of CSE to determine whether they are in compliance with the law.

As noted in my earlier reports, CSE provides the Government of Canada with foreign intelligence, which it obtains by gathering and analyzing foreign radio, radar and other electronic emissions. This is called signals intelligence or SIGINT. CSE also provides technical advice, guidance and service on the means of protecting the security of government telecommunications and aspects of electronic data processing. This is known as Information Technology Security or ITS.

Clearly, the work CSE performs is highly sensitive. The foreign intelligence it collects provides the government with valuable information about foreign and defence policy issues in response to intelligence priorities established by Cabinet.

The three-year term of my first mandate has now ended. In this, my third Annual Report, covering the period to March 31, 1999, I will discuss the activities of the past year but also reflect on the evolution of the review function for CSE since my appointment in 1996.

The knowledge gained and lessons learned during my first mandate will be instrumental in ensuring further progress during my second mandate, which the Minister of National Defence announced on June 15, 1999. The new mandate, which will be in force until June 19, 2002, maintains the elements of the first one and enhances one important element — the complaints function of my office. I am pleased with this change, which responds to concerns I raised in my past two annual reports. This development and its implications are described below.

As noted in last year's report, I am satisfied with the resources at my disposal and with my access to CSE. In carrying out my review activities, I have the support of two full-time staff people and several experts retained on contract. My views about CSE are based not only on my own observations but also on the hard work of people who know the intelligence community and are familiar with the complex technology that is part of its day-to-day environment.

Looking Back on the First Mandate

My original detailed mandate, established by Order in Council in 1996 pursuant to the *Inquiries Act*, was:

- to review the activities of CSE to determine whether they are in compliance with the law,
- to advise the Minister of National Defence and the Attorney General of Canada of any activity of CSE that I believe may not be in compliance with the law,
- not to review issues for which other avenues of redress are established by statute,
- to submit to the Minister of National Defence a report containing classified information when I consider it advisable, and
- to submit to the Minister an annual report in both official languages on my activities and findings for tabling in Parliament.

A copy of the original Order in Council is appended to this report as Annex A.

As might be expected, I know much more about CSE now than I did when I took on this challenge three years ago. As my staff and I have learned more, we have asked CSE officials for more detailed information. Our questions continue to probe matters related to the lawfulness of CSE's activities

in a very penetrating way. In return, we expect and receive increasingly detailed explanations, which we then assess in each instance to determine whether there is logical continuity.

During my first mandate, I reviewed the lawfulness of CSE's activities from several perspectives. Initially I decided to focus on the control and accountability measures in place in CSE. For example, I was pleased to note the presence of legal counsel on CSE's senior management team. These lawyers, assigned to CSE by the Department of Justice, advise on the lawfulness of CSE's existing and planned activities and play an important part in the organization's decision making. I observed as well that CSE is subject to the independent scrutiny of the courts, the Canadian Human Rights Commission, the Privacy Commissioner, the Information Commissioner, the Commissioner of Official Languages, and the Auditor General.

I also examined CSE's reporting relationships. In Parliament, the Minister of National Defence is answerable for all CSE's activities. The Minister is supported by two deputy ministers — the Deputy Minister of National Defence for administrative matters, and the Deputy Secretary to the Cabinet (Security and Intelligence) in the Privy Council Office for policy and operations.

Next, I examined CSE's internal policies and procedures, the processes for reviewing and improving them, and programs for training employees about them. In an organization such as CSE, which operates without legislation in a very sensitive area, policies and procedures that reinforce lawful behaviour are essential. Equally important are the organization's continuing efforts to improve its policies and procedures and ensure employees know and live up to them.

My staff also developed and refined procedures for examining and testing CSE's information holdings, to ensure that those holdings contain only information that CSE is authorized to retain. This testing program is described in more detail below.

Technology, Privacy and Review

CSE's signals intelligence work depends on sophisticated technology for its success. This presents challenges for the organization. On the one hand, operating in a field where technology is advancing rapidly, CSE must upgrade its technology constantly to meet the government's foreign intelligence requirements. On the other hand, the rapid pace of technological change presents CSE with a particular challenge in protecting the rights of Canadians, since new technologies can expand CSE's capabilities.

The sophistication of CSE's technology has led to speculation about the organization's capability to intercept the communications of Canadians. However, I have observed that CSE's activities are driven not by the capabilities of the technology it deploys but by its mandate to fulfil the foreign intelligence requirements established by the Government of Canada. My review and analysis indicate that CSE is not using its technology to target Canadian communications. In keeping with the policy of the government, CSE goes to considerable effort to avoid collecting Canadian communications.

Technology can, of course, be used to protect privacy. As CSE's technological capabilities progress, its ability to avoid collecting information that does not advance its foreign intelligence mandate increases. New technologies can help CSE improve intelligence collection and support the organization's lawfulness. I will continue to examine carefully CSE's use of technology in the months and years ahead.

The Effect of Review on CSE

In my last report, I cited a generally held view that observation prompts change. In other words, the very presence in an organization of external observers of performance can increase the internal commitment to improve that performance.

In the case of an intelligence agency, effective performance is a function of the professed values of the organization, the activities it undertakes to achieve results, and its commitment to hold itself accountable for both its values and its results.

During my first mandate I observed that the precept that observation prompts change applies to CSE. In my assessments of the agency, I examined not only CSE's activities but also its values, as articulated in its policies and procedures. I can confirm that the presence of a review function is contributing to the momentum for improvement and serves as a reminder to employees of the values that CSE has articulated.

A further benefit of the review function has been that CSE's employees, knowing independent reviewers have informed the public that CSE's activities are lawful, have been able to approach their jobs with more confidence and thus better serve the Government of Canada.

These, I believe, are important arguments in favour of a permanent review mechanism.

1998-99 Activities

Two major undertakings represented the bulk of my office's work this past fiscal year. The first revolved around testing the information in CSE's databases. The second involved research and information gathering in support of the complaints function, which has now been fully integrated into my new mandate.

Testing

During the period under review, my staff devoted considerable effort to testing CSE's signals intelligence databases. CSE analysts search these electronic files daily to identify intelligence that meets the government's foreign and defence priorities. They then process and distribute this intelligence to CSE's client departments and agencies within the government. My staff's unlimited access to these holdings, therefore, provides my office with a direct passageway into the principal product of CSE's SIGINT collection efforts — and the ideal mechanism to test the lawfulness of CSE's collection activities.

Our approach to testing remains a work in progress. It is under continual development and refinement, not only as our knowledge and understanding of CSE deepen, but also in response to technological advancements, changing collection practices and evolving intelligence priorities.

Our testing is directed at determining whether CSE acts in accordance with the fundamental principles of lawfulness and privacy. In conducting our tests, we are constantly aware of a series of facts about the organization. For example:

- CSE is both a collector of foreign communications intercepts and a recipient of communications intercepts collected by Second Parties;*
- CSE does not have the authority to target the communications of Canadians;
- Canadian communications can make their way into CSE's information holdings, since absolute exclusion is technically impossible at this time;
- CSE uses the technical means at its disposal to reduce the inadvertent interception of Canadian communications;

*Australia, New Zealand, United Kingdom, United States.

-
- CSE has policies and practices to address the safeguarding and proper handling of inadvertently collected Canadian communications in accordance with the laws of Canada, including the *Privacy Act*, the *Criminal Code* and the *Canadian Charter of Rights and Freedoms*.

These facts about CSE have led me to establish several objectives for our testing program, including:

- to determine whether CSE targets or possesses Canadian communications;
- to review and assess CSE's adherence to policies and practices on the handling of the communications of Canadians in accordance with the laws of Canada; and
- to assess the comprehensiveness and effectiveness of the technical means used to safeguard the privacy of Canadian communications.

As a result of our testing program, my staff has regular contact with CSE employees and continuous access to the organization's information holdings. The testing function complements and verifies my office's other methods for assessing compliance issues related to lawfulness and privacy. And the very presence of my staff as they conduct our tests onsite at CSE is a visible reminder to CSE's operational staff of the legal boundaries within which they must operate.

The Complaints Function

Readers of my two earlier reports will recall that I expressed concern about complaints. In brief, while the 1996 Order in Council authorized me to receive complaints about CSE's mandated activities, I lacked the authority to report to individual complainants about my findings. Instead, I had to suggest to complainants that they draw their own conclusions about my findings from the contents of my annual reports.

This matter is now rectified. The Order in Council that will guide my activities from June 19, 1999 to June 19, 2002 includes a provision by which I may receive, examine and report back on a complaint laid by any individual who is a Canadian citizen or a permanent resident of Canada. I look forward to operating under these new terms of reference. Although the comprehensiveness of the work of my office will not change, I am now able to respond directly to individuals about my findings. It remains my intention, however, not to examine allegations of wrongdoing with respect to incidents that took place before my original appointment on June 19, 1996.

In anticipation of this enhancement, in August 1998, my office sought advice and embarked on a series of studies to determine the budgetary, staffing and administrative implications of an integrated complaints function. I wanted to learn as well about the best practices of others whose responsibilities include receiving and examining complaints and responding to complainants, both in Canada and abroad.

Although I have received several complaints since 1996, I have no way of knowing whether the number or nature of complaints will change with the revised mandate. However, I do have a few objectives for the function itself. I want an approach based on sound systems and practices that can be expanded or contracted as needed, depending on the number of files involved. I want to ensure that current dispute resolution mechanisms and practices are featured. I want to avoid creating an administrative burden for CSE and my office and to keep bureaucracy and paperwork to a minimum.

When we began to examine other complaints functions, it was clear that any study would require a careful focus, since myriad examples exist. We chose to review the policies and practices of six other federal offices that handle complaints and

investigations resulting from the actions or inactions of another agency or department of government. We also studied how complaints are handled by other jurisdictions, including the United Kingdom, Australia and New Zealand.

I am grateful to many people who gave generously of their time and experience, including officials at the offices of the Correctional Investigator, the Information Commissioner, the Official Languages Commissioner, the Privacy Commissioner, the RCMP Public Complaints Commission, and the Security Intelligence Review Committee. As a result of this effort, I expect that the transition to my new mandate will be a smooth one.

Other Activities

In August 1998, I testified before the Special Senate Committee on Security and Intelligence, chaired by Senator William M. Kelly. In my remarks, I described the work of my office and the options for long-term review of CSE. I was pleased with the Committee's recommendation, in its January 1999 report, that CSE should have its own Act of Parliament and that the legislation should provide for a permanent and separate review body for CSE.

Back in 1996, the Auditor General conducted an audit of the Canadian intelligence community. This past December, he issued a short follow-up report to the 1996 study. In his generally positive comments about the community's response to his report, he reiterated his view that legislation for CSE could be of value.

Shortly after the end of the 1998-99 fiscal year, CSE sponsored its first ever Law Day. The event coincided with other Law Day celebrations across the country held annually to mark the anniversary of Canada's Charter of Rights and Freedoms. I was pleased to participate in the event at CSE, where I

spoke to a large gathering of employees about the role of my office in determining whether the activities of CSE are lawful. I noted that the creation of a review function for CSE grew out of Canadians' increased awareness of the rights of individuals, an awareness reflected in the Charter. The recent creation of review functions for security and intelligence agencies in similar democratic countries, such as the United Kingdom, Australia and New Zealand, suggests that our experience in Canada is not unique.

Budget and Staff

When the government established my office, it allocated an annual budget of approximately \$500,000, including salaries. In addition to paying for the usual costs of running an office, I chose to hire two full-time staff and to bring in several subject-area specialists on contract. This approach allowed me to have at hand the range of expertise required to fulfil my mandate.

I can report that total spending for the three years was \$1.117 million, well within the budget. Annex B to this report provides a statement of my expenditures over the course of the first mandate.

1998-99 Findings

While our methods for reviewing CSE's activities have become more sophisticated and have allowed us to delve more deeply into the organization, our findings have not changed. Based on the results of our review and analysis, I am of the opinion that CSE has acted lawfully in the performance of its mandated activities during the 1998-99 review period. I am also satisfied that CSE has not targeted the communications of Canadian citizens or permanent residents of Canada.

During 1998-99, I submitted three classified reports to the Minister of National Defence, bringing to seven the number of such reports submitted during

my first mandate. These reports examined some aspect of CSE's SIGINT and ITS activities. None of my classified reports brought to the Minister's attention incidents of unlawful activity on the part of CSE.

Operational Policy Revisited

In my last report, I noted that I had reviewed the operational policies in place at CSE to determine whether they provided adequate guidance to employees in the performance of their duties. I also indicated my particular interest in policies related to privacy issues.

I concluded then that there was an appreciable amount of sound operational policy in place at CSE and that there were no policy gaps on matters of lawfulness or privacy. I did observe, however, that policy was not always at the right organizational level. While this is not always an easy call to make, a useful test is to examine whether the level of the individual with the authority to change a policy is appropriate to the importance of the policy. In other words, the most important policies should be alterable only at the highest levels of authority.

During this reporting year, CSE undertook to restructure its internal policy development process. With the approval and support of the senior management team, CSE adopted a new framework for policy authority, accountability and coordination. The framework, which was approved in late 1998, identifies the appropriate level of authority for various policies and provides a desirable level of operational flexibility in support of day-to-day activities.

This is a welcome initiative and, once it is fully in place, I plan to examine its effect on the policies and derivative practices that address issues of lawfulness.

The Review Function

On several occasions, I have expressed the view that CSE should have its own legislation. Legislation would put the agency on a firm footing by articulating its mandate and powers and its relationships with Parliament, the Government, and the Minister of National Defence. It would seem reasonable to expect that provisions for a permanent review mechanism would also be included.

Some observers have suggested that the activities of Canada's foreign signals intelligence agency and its domestic security intelligence agency could be examined by the same review mechanism. In defence of this idea, they cite such advantages as economies of scale. I am not a supporter of this proposal, however, for a number of reasons.

First, the mandates of the two agencies in question are markedly different: one provides the government with information and advice on threats to national security, while the other provides foreign signals intelligence in support of the government's foreign and defence policies. Second, the agencies report to Parliament through different ministers of the Crown, as do the bodies that now review their activities.

These are not the most compelling reasons, however.

In the three years I have spent as CSE Commissioner, I have concluded that a fundamental distinction must be made between the activities of a domestic intelligence agency and those of a foreign intelligence agency such as CSE. This distinction must also be reflected in both the ethos and the undertakings of the bodies responsible for reviewing them. The need to distinguish between the two stems directly from the unique relationship between each agency and the citizens of the country it serves.

To fulfil its mandate, a domestic intelligence agency must maintain constant contact with the citizens of the nation, through programs of varying degrees of intrusiveness, designed to collect intelligence about threats to security within its borders. The mandate of its corresponding review body must therefore be broad-based, reflecting the reality that this relationship is sensitive, ongoing, and at the core of the agency's activities.

CSE, on the other hand, has no such relationship with Canadians. It relies on a variety of sophisticated technologies to fulfil its SIGINT mandate. Its activities serve the interests of Canadians by collecting intelligence from outside Canada's borders in relation to the government's foreign and defence priorities. Appropriately, my review mandate relates directly to the lawfulness of CSE's activities.

I have concluded that the most important feature of any review mechanism is to provide assurance to the appropriate minister, to Parliament and, ultimately, to the public. This assurance should be based on careful examination of the activities at the heart of the agency under review. In this regard, I believe the current review arrangements, although perhaps not the ultimate review solution, serve Canadians well.

Farewell

During the course of the period under review, Mr. Stewart Woolner, Chief of CSE, retired from the public service. During his 37 years with CSE, Mr. Woolner oversaw many significant changes in the organization and its operating environment, including the introduction of my review function. I want to take this opportunity to express my appreciation for his cooperation and professionalism and to signal his unique dedication to the work CSE performs on behalf of the people of Canada.



CANADA

PRIVY COUNCIL • CONSEIL PRIVÉ

P.C. 1996-899

June 19, 1996

His Excellency the Governor General in Council, on the recommendation of the Minister of National Defence, pursuant to Part II of the *Inquiries Act*, hereby authorizes the Minister of National Defence ("Minister"):

(a) to appoint the Honourable Claude Bisson of Montreal, Quebec, for a period of three years, as a commissioner ("Commissioner") to review the activities of the Communications Security Establishment ("CSE") for the purpose of determining whether those activities are in compliance with the law;

(b) to direct the Commissioner to submit to the Minister, once each year and in both official languages, a report on the Commissioner's activities and findings that are not of a classified nature, which report the Minister will table in Parliament;

(c) to authorize the Commissioner, at any time the Commissioner considers it advisable, to submit a report containing classified information to the Minister;

(d) to direct the Commissioner to advise the Minister and the Attorney General of Canada of any activity of CSE that the Commissioner believes may not be in compliance with the law;

(e) to direct the Commissioner not to review issues for which other avenues of redress are established by statute;

.../2

- 2 -

(f) to require that the Commissioner and all persons engaged on his behalf take an oath of secrecy and comply with all applicable government security requirements;

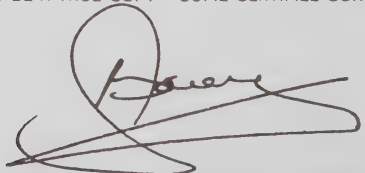
(g) to direct the Commissioner, before submission of any report to the Minister, to consult with the Deputy Clerk, Security and Intelligence, and Counsel at the Privy Council Office for the purpose of ensuring compliance with all security requirements and preservation of the secrecy of sources of security and intelligence information and of the security of information provided to Canada in confidence by other nations;

(h) to authorize the Commissioner to engage the services of such staff and technical advisors as he considers necessary to assist him in his review, at such rates of remuneration and reimbursement as may be approved by the Treasury Board;

(i) to fix the remuneration of the Commissioner at the per diem rate set out in the schedule hereto, which rate is within the range of \$400 to \$500; and

(j) to authorize that the Commissioner be reimbursed for his actual transportation expenses and a non-accountable living allowance of up to \$175 per diem while in travel status away from his normal place of residence in connection with the conduct of this review.

CERTIFIED TO BE A TRUE COPY - COPIE CERTIFIÉE CONFORME



CLERK OF THE PRIVY COUNCIL - LE GREFFIER DU CONSEIL PRIVÉ

Statement of Expenditures

Standard Object Summary

	<u>1996-97*</u>	<u>1997-98</u>	<u>1998-99</u>
01 Salaries and Wages	97,935	147,623	160,926
02 Transportation and Telecommunications	13,688	24,789	16,755
03 Information	4,916	7,977	10,725
04 Professional and Special Services	65,975	124,787	235,192
05 Rentals	4,235	35,525	59,169
06 Purchased Repair and Maintenance	23,113	622	0
07 Materials and Supplies	5,937	5,984	4,595
09 Acquisition of Equipment	16,980	17,226	32,278
12 Miscellaneous	<u>1</u>	<u>24</u>	<u>39</u>
	232,780	364,556	519,679

* represents partial year

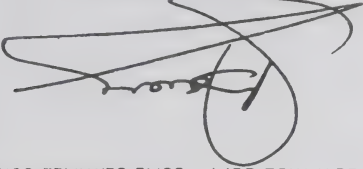
État des dépenses

Sommaire des articles courants

	1996-1997*	1997-1998	1998-1999
01 Traitements et salaires	97 935	147 623	160 926
02 Transports et communications	13 688	24 789	16 755
03 Information	4 916	7 977	10 725
04 Services professionnels et spéciaux	65 975	124 787	235 192
05 Locations	4 235	35 525	59 169
06 Achat de services de réparation et d'entretien	23 113	622	0
07 Fournitures et approvisionnements	5 937	5 984	4 595
09 Acquisition de matériel	16 980	17 226	32 278
12 Dépenses diverses	1	24	39
	232 780	364 556	519 679

* représente une partie de l'année

CLERK OF THE PRIVY COUNCIL - LE GREFFIER DU CONSEIL PRIVÉ



CERTIFIED TO BE A TRUE COPY - COPIE CERTIFIÉE CONFORME

f) à exiger que le commissaire et toutes les personnes engagées pour son compte prononcent un serment de discrétion et se conforment à toutes les exigences du gouvernement applicables au secret;

g) à ordonner au commissaire, avant la présentation de tout rapport au ministre, de consulter le sous-greffier, sécurité et renseignement et conseiller juridique au Bureau du Conseil privé en vue de veiller à ce que toutes les exigences visant la sécurité soient respectées et que la confidentialité des sources de sécurité et de renseignements secrets et la sécurité de l'information fournie au Canada par d'autres nations à titre confidentiel soit protégée;

h) à autoriser le commissaire à retenir les services des experts et du personnel qu'il juge nécessaires pour l'assister dans son enquête, aux taux de rémunération que peut approuver le Conseil du Trésor;

i) à fixer la rémunération du commissaire au taux journalier établi dans l'annexe ci-jointe, lequel taux se situe dans l'échelle de 400 \$ à 500 \$;

j) à autoriser le remboursement des frais de transports réels du commissaire ainsi qu'une allocation de subsistance non à justifier allant jusqu'à 175 \$ par jour lors de son déplacement à l'extérieur de son lieu de résidence habituel dans l'exercice des fonctions de cette enquête.

.../2

- e) à ordonner au commissaire de ne pas examiner les questions pour lesquelles il existe d'autres recours statutaires;
- d) à ordonner au commissaire d'aviser le ministre et le procureur général du Canada au sujet de toute activité du CST qu'il estime ne pas être conforme à la loi;
- c) à autoriser le commissaire à soumettre au ministre tout rapport classifié, aux moments où il le juge indiqué;
- b) à ordonner au commissaire de présenter au ministre, une fois l'an et dans les deux langues officielles, un rapport sur ses activités et ses constatations qui ne sont pas de nature classifiée, lequel rapport sera déposé par le ministre auprès du Parlement;
- a) à nommer l'honorable Claude Bisson, de Montréal (Québec), pour une période de trois ans, commissaire pour faire enquête sur les activités du Centre de la sécurité des télécommunications (« CST ») en vue de déterminer si ces activités sont conformes à la loi;
- Sur recommandation du ministre de la Défense nationale et en vertu de la partie II de la Loi sur les enquêtes, Son Excellence le Gouverneur général en conseil autorise le ministre de la Défense nationale (ci-après appelé le « ministre ») :

PRIVY COUNCIL • CONSEIL PRIVÉ



CANADA

C.P. 1996-899
19 juin 1996

Adieu

sur les menaces présentées à la sécurité sur son territoire. Le mandat de l'organisme d'examen correspondant doit donc être large, compte tenu du fait que ce rapport est délicat et permanent et se situe au cœur des activités du service.

Le CST, pour sa part, n'entretenait pas ce genre de rapport avec les Canadiens. Il s'appuie sur une variété de moyens techniques sophistiqués pour s'acquitter de son mandat en matière de SIGINT. Ses activités servent les intérêts des Canadiens en ce sens qu'il recueille des renseignements provenant de l'extérieur du Canada aux fins des priorités du gouvernement en matière d'affaires étrangères et de défense. Fort à propos, mon mandat d'examiner ses activités porte directement sur leur légalité.

J'ai conclu que la caractéristique la plus importante de tout mécanisme d'examen consiste à rassurer le ministre compétent, le Parlement et, en fin de compte, le public. Il faut pour cela examiner soigneusement les activités qui sont au cœur de l'organisme concerné. Dans ce sens, je pense que les mécanismes d'examen actuels, s'ils n'offrent peut-être pas la solution suprême, servent bien les Canadiens.

Au cours de la période à l'examen, M. Stewart Woolner, chef du CST, a pris sa retraite de la fonction publique. Pendant les 37 années qu'il a passées au CST, M. Woolner a présidé à de nombreux changements importants qui ont été apportés à l'organisme et à son cadre opérationnel, dont l'instauration de ma fonction d'examen. Je profite de l'occasion que me fournit ce rapport pour le remercier de sa coopération et de son professionnalisme et pour souligner son dévouement exceptionnel au travail qu'il accomplit le CST pour le compte de la population du Canada.

Certains observateurs ont donné à entendre que les activités de l'organisme canadien de collecte de renseignements électromagnétiques sur l'étranger et de son service intérieur de renseignement de sécurité pourraient être examinées par le même groupe de personnes. Ils citent, à l'appui de cette idée, des avantages comme les économies d'échelle. Je n'appuie cependant pas cette proposition et ce, pour diverses raisons.

Premièrement, les mandats des deux organismes en question sont sensiblement différents : l'un fournit au gouvernement de l'information et des conseils sur les menaces à la sécurité nationale, tandis que l'autre fournit des renseignements sur les transmissions électroniques de pays étrangers à l'appui des politiques étrangères et de défense du gouvernement. Deuxièmement, ils font rapport au Parlement par l'entremise de ministres différents, tout comme les organismes qui examinent actuellement leurs activités.

À mon sens, toutefois, ces raisons ne sont pas les plus impératives.

Au cours des trois années pendant lesquelles j'ai exercé la charge de commissaire du CST, j'ai conclu qu'il faut faire une distinction fondamentale entre les activités d'un service de renseignement intérieur et celles d'un organisme de renseignements sur l'étranger comme le CST. Cette distinction doit en outre se refléter dans le génie et les travaux des groupes chargés d'examiner ces activités. Le besoin de les distinguer découle directement des rapports uniques qui existent entre chacun des organismes et les citoyens du pays qu'ils servent.

Pour remplir son mandat, un service de renseignement intérieur doit maintenir un contact constant avec les citoyens du pays au moyen de programmes comportant des degrés divers d'intrusion, afin de recueillir des renseignements

La fonction d'examen

J'ai déclaré à quelques reprises être d'avis que le CST devrait disposer de sa propre loi habilitante. Une telle loi l'assoirait sur une base solide en énonçant expressément son mandat et ses pouvoirs ainsi que ses rapports avec le Parlement, le gouvernement et le ministre de la Défense nationale. Il semblerait raisonnable de s'attendre à ce qu'elle renferme également des dispositions prévoyant un mécanisme d'examen permanent.

La vie privée. J'avais toutefois fait remarquer que les politiques ne se trouvaient pas toujours au bon palier de l'organisation. Si cette question n'est pas toujours facile à trancher, il est utile d'examiner si le niveau de la personne autorisée à modifier une politique est proportionné à l'importance de celle-ci. Autrement dit, les politiques les plus importantes devraient seulement pouvoir être modifiées au plus haut niveau.

Au cours de l'année visée dans le présent rapport, le CST a entrepris de restructurer son processus interne d'élaboration des politiques. Fort de l'approbation et de l'appui soutenu de la haute direction, il a adopté un nouveau cadre de pouvoirs, de responsabilités et de coordination touchant les politiques. Ce cadre, qui a été approuvé à la fin de 1998, définit le niveau d'autorité approprié pour diverses politiques et procure un degré souhaitable de souplesse opérationnelle pour les activités quotidiennes.

Il s'agit là d'une initiative bienvenue et, une fois qu'elle aura été pleinement mise en œuvre, je me propose d'examiner son effet sur les politiques et les pratiques connexes visant les questions de légalité.

Réexamen de la politique opérationnelle

Constatations faites en 1998-1999

Je suis à même de signaler que nos dépenses totales, des trois années ont été de 1,17 million de dollars, ce qui est nettement dans les limites de notre budget. On trouvera à l'annexe B un état des dépenses de mon bureau au cours de mon premier mandat.

Si nos méthodes d'examen des activités du CST se sont raffînées et nous ont permis de scruter celles-ci plus à fond, nos constatations n'ont pas changé. En me fondant sur les résultats de notre examen et de notre analyse, je suis d'avis que, au cours de la période d'examen 1998-1999, le CST a agi légalement dans l'exercice des activités dont il est chargé. Je suis par ailleurs convaincu qu'il n'a pas ciblé les communications de citoyens canadiens ni de résidents permanents du Canada.

Au cours de l'année 1998-1999, j'ai présenté trois rapports classifiés au ministre de la Défense nationale, ce qui a porté à sept le nombre des rapports de cette nature que je lui ai communiqués au cours de mon premier mandat. Ceux-ci portaient sur certains aspects des activités de SIGINT et de STI du CST. Aucun de ces rapports n'a signalé au Ministre de cas d'activité illégale de la part du CST.

Je mentionnais dans mon dernier rapport que j'avais passé en revue les politiques opérationnelles en place au CST afin de déterminer si elles procuraient des conseils suffisants aux employés pour leur permettre d'exercer leurs fonctions. Je signalais en outre mon intérêt particulier pour les politiques relatives aux questions de protection de la vie privée.

J'avais alors conclu que le CST disposait d'une quantité appréciable de politiques opérationnelles solides et qu'elles ne présentaient aucune lacune sur le plan de la légalité ni sur celui de la protection de

Budget et personnel

En 1996, le vérificateur général avait procédé à une vérification des activités de la communauté canadienne du renseignement. En décembre dernier, il a publié un court rapport de suivi de son étude de 1996. Dans ses remarques généralement positives au sujet de la réaction de la communauté à son rapport, il a réitéré son opinion selon laquelle une loi devant régir le CST pourrait être utile.

Peu après la fin de l'année financière 1998-1999, le CST a parrainé la première Journée du droit de son histoire. Cet événement a coïncidé avec les autres manifestations semblables tenues annuellement un peu partout au pays pour souligner l'anniversaire de la Charte canadienne des droits et libertés. J'ai été heureux de participer à la manifestation au CST, où j'ai exposé à un groupe important d'employés le rôle joué par mon bureau pour déterminer si les activités de leur organisme sont légales. J'ai signalé que la création de ma charge était née de la sensibilisation accrue des Canadiens aux droits de la personne, sensibilisation qui se reflétait dans la Charte. La création récente de fonctions d'examen des activités des services de sécurité et de renseignement de pays démocratiques similaires, comme le Royaume-Uni, l'Australie et la Nouvelle-Zélande, indique que l'expérience du Canada n'est pas unique.

Lorsque le gouvernement a établi mon bureau, il y a affecté un budget annuel d'environ 500 000 \$, salaires compris. En plus de payer les coûts habituels de fonctionnement d'un bureau, j'ai choisi d'embaucher deux employés à plein temps et de retenir par contrat les services de plusieurs spécialistes de questions particulières. Cette façon de procéder m'a permis de disposer de l'ensemble des compétences nécessaires pour m'acquitter de mon mandat.

Autres activités

Au mois d'août 1998, j'ai témoigné devant le Comité spécial du Sénat sur la sécurité et les services de renseignement, que préside le sénateur William M. Kelly. J'ai exposé dans mes remarques le travail de mon bureau et les formules possibles pour l'examen à long terme des activités du CST. Je me suis réjoui de la recommandation formulée par le Comité dans son rapport de janvier 1999, à savoir que le CST devrait être régi par une loi particulière et que celle-ci devrait prévoir un organisme permanent et distinct d'examen de ses activités.

Lorsque nous avons commencé à examiner d'autres fonctions relatives aux plaintes, il est apparu clairement qu'il fallait soigneusement délimiter notre étude, car les exemples existants sont innombrables. Nous avons donc décidé d'étudier les politiques et pratiques de six autres bureaux fédéraux qui traitent les plaintes résultant des actes ou de l'inaction de quelque autre organisme ou ministère de l'État et effectuent les enquêtes correspondantes. Nous avons en outre examiné comment d'autres pays, dont le Royaume-Uni, l'Australie et la Nouvelle-Zélande, traitent les plaintes.

Je suis reconnaissant envers de nombreuses personnes qui ont donné généreusement de leur temps et fait part de leur expérience à mon personnel, notamment les fonctionnaires des bureaux de l'enquêteur correctionnel, du commissaire à l'information, du commissaire aux langues officielles, du commissaire à la protection de la vie privée, de la Commission des plaintes du public contre la Gendarmerie royale du Canada et du Comité de surveillance des activités de renseignement de sécurité. Je prévois que, grâce à ce travail, la transition à mon nouveau mandat se fera en douceur.

Cette question est maintenant réglée. Le décret qui orientera mes activités du 19 juin 1999 au 19 juin 2002 renferme une disposition selon laquelle je pourrai recevoir et étudier toute plainte formulée par n'importe quel citoyen ou résident permanent du Canada et lui faire rapport de mes constatations. J'ai hâte d'opérer dans le cadre de ce nouveau mandat. Le caractère détaillé du travail de mon bureau ne changera pas, mais je serai désormais en mesure de rendre compte de mes constatations directement aux intéressés. J'entends toujours, cependant, ne pas examiner d'allégations de méfaits relatives à des incidents survenus avant ma nomination initiale du 19 juin 1996.

En prévision de cette amélioration, au mois d'août 1998, mon bureau a sollicité des avis et entrepris une série d'études destinées à déterminer les incidences qu'aurait l'intégration d'une fonction relative aux plaintes sur notre budget, sur nos besoins en personnel et sur nos tâches administratives. Je voulais également me renseigner sur les meilleures pratiques employées par d'autres organismes chargés, entre autres choses, de recevoir et d'étudier des plaintes, et de répondre aux plaignants, tant au Canada qu'à l'étranger.

J'ai reçu plusieurs plaintes depuis 1996, mais je n'ai aucun moyen de savoir si la révision de mon mandat modifiera le nombre ou la nature de celles qui me seront adressées à l'avenir. J'ai toutefois quelques objectifs pour la fonction elle-même. Ainsi, je veux pouvoir aborder les plaintes en me fondant sur des systèmes et des pratiques solides qui pourront être élargis ou comprimés au besoin, selon le nombre de dossiers à traiter. Je veux m'assurer qu'on aura recours aux mécanismes actuels de règlement des différends et aux usages courants en la matière. Et je veux éviter de créer un fardeau administratif pour le CST et pour mon bureau, et réduire au minimum les tracasseries administratives et la paperasserie.

La fonction relative aux plaintes

Les lecteurs de mes deux rapports précédents se rappelleront que j'ai exprimé une préoccupation au sujet des plaintes. En bref, si le décret de 1996 m'autorisait à recevoir des plaintes se rapportant aux activités dont le CST est chargé, je n'avais pas le pouvoir de faire rapport de mes constatations aux plaignants. Je devais plutôt leur conseiller de tirer leurs propres conclusions sur celles-ci à la lumière du contenu de mes rapports annuels.

L'existence de ce programme de vérification fait que mon personnel est en contact régulier avec les employés du CST et a continuellement accès à ses fonds de renseignements. Les vérifications complètent les autres méthodes employées par mon bureau pour évaluer les questions de conformité liées à la légalité et à la protection de la vie privée, et procurent un moyen de les contrôler. Et la présence de membres de mon personnel au CST même pour effectuer ces vérifications rappelle concrètement à ses employés opérationnels les limites juridiques qu'ils doivent respecter dans leur travail.

- déterminer si le CST cible ou possède des communications canadiennes;
 - examiner et évaluer le respect, par le CST, des politiques et pratiques relatives au traitement des communications de Canadiens conformément aux lois du Canada;
 - évaluer la complétude et l'efficacité des moyens techniques utilisés pour protéger le caractère privé des communications canadiennes.
- Compte tenu de ces faits, j'ai établi plusieurs objectifs pour notre programme de vérification, dont les suivants :

Notre méthode de vérification évolue constamment. Nous l'améliorons et la raffinons sans cesse, non seulement à mesure que notre connaissance et notre compréhension du CST s'approfondissent, mais encore en réponse aux progrès technologiques, à la modification des pratiques de collecte et à l'évolution des priorités en matière de renseignement.

Nos vérifications visent à déterminer si le CST agit conformément aux principes fondamentaux de la légalité et de la protection de la vie privée. Lorsque nous les effectuons, nous avons constamment à l'esprit un ensemble de faits au sujet de l'organisme. Par exemple :

- non seulement le CST recueille des renseignements sur des pays étrangers en interceptant leurs communications, mais encore il reçoit des communications interceptées par des Secondes Parties*;

- le CST n'est pas autorisé à cibler les communications de Canadiens;

- des communications canadiennes peuvent se retrouver dans les fonds de renseignements du CST, car il est techniquement impossible, à l'heure actuelle, de les exclure totalement;

- le CST utilise les moyens techniques à sa disposition pour réduire l'interception involontaire de communications canadiennes;

- le CST possède des politiques et des pratiques destinées à assurer la protection et le traitement approprié des communications canadiennes recueillies involontairement, conformément aux lois du Canada, dont la *Loi sur la protection des renseignements personnels*, le *Code criminel* et la *Charte canadienne des droits et libertés*.

*Australie, États-Unis, Nouvelle-Zélande et Royaume-Uni.

Vérification

Activités de l'année 1998-1999

d'une fonction d'examen contribue au mouvement d'amélioration et sert à rappeler aux employés les valeurs que le CST s'est données.

Autre avantage de la fonction d'examen : les employés du CST, sachant que des observateurs indépendants ont informé le public de la légalité de ses activités, ont été à même d'aborder leur travail avec plus d'assurance et, par conséquent, de mieux servir le gouvernement du Canada.

Ce sont là, à mon sens, des arguments importants en faveur de l'instauration d'un mécanisme d'examen permanent.

Deux grandes entreprises ont constitué la majeure partie des travaux de mon bureau au cours de la dernière année financière. La première a touché la vérification des renseignements contenus dans les bases de données du CST. La seconde a consisté à faire des recherches et à recueillir des renseignements à l'appui de la fonction relative aux plaintes, qui est maintenant pleinement intégrée à mon nouveau mandat.

Au cours de la période à l'étude, mon personnel a consacré énormément d'énergie à la vérification des bases de données de renseignements électromagnétique du CST. Les analystes du CST examinent en détail ces fichiers électroniques quotidiennement pour trouver des renseignements qui répondent aux priorités du gouvernement en matière d'affaires étrangères et de défense. Ils traitent ensuite ces renseignements et les diffusent aux ministères et organismes clients du CST au sein de l'administration fédérale. L'accès illimité de mon personnel à ces fonds de renseignements assure donc à mon bureau un contact direct avec le principal produit du travail de collecte de SIGINT du CST, ainsi que le mécanisme idéal pour vérifier la légalité de ses activités de collecte.

L'effet de l'examen sur le CST

Canada, et non pas les capacités de la technologie qu'il met en œuvre. Mon examen et mon analyse révélèrent qu'il n'utilise pas sa technologie pour cibler des communications canadiennes. Conformément à la politique du gouvernement, le CST déploie des efforts considérables pour éviter de recueillir des communications canadiennes.

On peut, bien sûr, utiliser la technologie pour protéger la vie privée. À mesure que les moyens technologiques du CST s'améliorent, sa capacité d'éviter de recueillir des renseignements qui ne cadrent pas avec son mandat touchant les renseignements sur l'étranger augmente. Les nouvelles technologies peuvent l'aider à améliorer sa collecte de renseignements et soutenir en même temps la légalité de ses activités. Au cours des mois et des années à venir, j'entends continuer à examiner soigneusement l'utilisation que le CST fait de la technologie.

Dans mon dernier rapport, j'ai fait allusion à l'opinion générale selon laquelle l'observation suscite le changement. Autrement dit, la présence même, dans une organisation, de personnes de l'extérieur qui observent son rendement peut accroître l'engagement interne à améliorer celui-ci.

Dans le cas d'un organisme de renseignement, le rendement réel dépend des valeurs professées par cet organisme, des activités auxquelles il s'adonne pour atteindre les résultats, et de son engagement à assumer la responsabilité à la fois de ses valeurs et de ses résultats.

Au cours de mon premier mandat, j'ai constaté que la maxime selon laquelle l'observation suscite le changement s'applique au CST. Dans mes évaluations de l'organisme, j'ai examiné non seulement ses activités, mais aussi ses valeurs, telles qu'elles se traduisent dans ses politiques et ses méthodes. Je peux confirmer que l'existence

Technologie, protection de la vie privée et examen

J'ai ensuite examiné les politiques et méthodes internes du CST, les processus établis pour les réviser et les améliorer, et les programmes prévus pour former les employés à leur sujet. Dans un organisme comme le CST, qui exerce son activité sans cadre législatif dans un domaine très délicat, les politiques et méthodes propres à renforcer un comportement conforme à la loi sont essentielles. Les efforts déployés par l'organisme pour améliorer constamment ses politiques et ses méthodes et faire en sorte que les employés les connaissent et s'y conforment sont tout aussi importants.

Mon personnel a par ailleurs élaboré et raffiné des procédures afin d'examiner et de vérifier les fonds de renseignements du CST pour s'assurer que ceux-ci contiennent seulement les renseignements que le CST est autorisé à conserver. Ce programme de vérification est décrit plus en détail plus loin.

Le succès des travaux de renseignement

électromagnétique du CST repose sur une technologie sophistiquée. Cela pose des défis à l'organisme. En effet, d'une part, il œuvre dans un domaine où la technologie évolue rapidement, de sorte qu'il doit mettre constamment ses moyens techniques à niveau afin de répondre aux besoins du gouvernement en matière de renseignements sur l'étranger. D'autre part, la rapidité de l'évolution technologique lui présente un défi particulier pour ce qui est de protéger les droits des Canadiens, car les nouvelles technologies peuvent accroître ses moyens d'action.

Je sais que le degré de perfectionnement de la technologie du CST a amené certaines personnes à s'interroger sur sa capacité d'intercepter les communications de Canadiens. Toutefois, j'ai constaté que le moteur des activités du CST est son mandat de répondre aux besoins de renseignements sur l'étranger établis par le gouvernement du

Le texte du décret est reproduit à l'annexe A du présent rapport.

Comme on peut le supposer, j'en sais beaucoup plus long au sujet du CST que lorsque j'ai assumé ma charge il y a trois ans. À mesure que mon personnel et moi-même avons appris plus de choses, nous avons demandé des renseignements plus détaillés aux responsables du CST. Au moyen de nos questions, nous continuons de scruter de façon approfondie des affaires liées à la légalité des activités du CST. Nous attendons et recevons en retour des explications de plus en plus détaillées que nous étudions dans chaque cas afin de déterminer s'il existe une continuité logique.

Au cours de mon premier mandat, j'ai examiné la légalité des activités du CST sous plusieurs angles. J'avais décidé au début de me concentrer sur les mesures de contrôle et de responsabilisation en place au CST. Par exemple, j'ai constaté avec plaisir que l'équipe de la haute direction de l'organisme comprenait des conseillers juridiques. Ceux-ci, affectés au CST par le ministère de la Justice, donnent des avis sur la légalité des activités présentes et prévues de l'organisme et prennent une part importante à ses décisions. J'ai en outre constaté que le CST est soumis à l'examen indépendant des tribunaux, de la Commission canadienne des droits de la personne, du commissaire à la protection de la vie privée, du commissaire à l'information, du commissaire aux langues officielles et du vérificateur général.

J'ai aussi examiné la structure de rapports du CST. Au Parlement, le ministre de la Défense nationale est comptable de toutes les activités de l'organisme. Il est appuyé par deux sous-ministres, soit le sous-ministre de la Défense nationale pour les questions administratives et le sous-secrétaire du Cabinet (Sécurité et Renseignement), du Bureau du Conseil privé, pour ce qui est de la politique et des opérations.

Coup d'œil rétrospectif sur le premier mandat

suitant :

Mon mandat initial détaillé, établi par décret en 1996 en vertu de la *Loi sur les enquêtes*, était le

Comme je le signalais dans mon rapport de l'année dernière, je suis satisfait des ressources mises à ma disposition et de l'accès que j'ai au CST. Je dispose, pour m'acquitter de mes activités d'examen, de deux employés à plein temps et de plusieurs experts engagés par contrat. Mes opinions au sujet du CST se fondent non seulement sur mes propres observations, mais aussi sur le travail ardu de personnes qui connaissent la communauté du renseignement ainsi que la technologie complexe qui fait partie de son contexte quotidien.

les éléments du premier et en renforce un qui est important, soit ma fonction relative aux plaintes. Je suis heureux de ce changement, qui correspond à des préoccupations soulevées dans mes deux rapports précédents. J'exposerais plus loin ce fait nouveau et ses incidences.

- examiner les activités du CST en vue de déterminer si elles sont conformes à la loi;
- informer le ministre de la Défense nationale et le procureur général du Canada de toute activité du CST qui n'apparaît non conforme à la loi;
- ne pas examiner les questions pour lesquelles il existe d'autres recours prévus par des lois;
- présenter au ministre de la Défense nationale des rapports contenant des renseignements classifiés lorsque je le juge à propos;
- présenter au Ministre un rapport annuel de mes activités et de mes constatations rédigé dans les deux langues officielles, pour dépôt au Parlement.

Le 19 juin 1996, le ministre de la Défense nationale m'a nommé au poste de commissaire du Centre de la sécurité des télécommunications (CST) pour un mandat de trois ans et m'a chargé d'examiner les activités de l'organisme en vue de déterminer si elles sont conformes à la loi.

Comme je l'ai mentionné dans mes rapports précédents, le CST fournit au gouvernement du Canada des renseignements sur des pays étrangers, qu'il obtient en recueillant et en analysant leurs transmissions électroniques par radio, par radar ou par d'autres moyens. C'est ce qu'on appelle le renseignement électromagnétique, ou SIGINT. Le CST fournit en outre des avis, des conseils et des services techniques sur les moyens de protéger la sécurité des télécommunications gouvernementales et certains aspects du traitement électronique de données. On désigne cette activité sous le titre de sécurité des technologies de l'information, ou STI.

Le travail du CST est manifestement très délicat. Les renseignements qu'il recueille sur l'étranger procurent au gouvernement une information précieuse sur les questions de politique étrangère et de défense, en réponse aux priorités établies par le Cabinet en matière de renseignement.

Les trois années de mon premier mandat sont maintenant achevées. Dans ce troisième rapport annuel, qui porte sur la période prenant fin le 31 mars 1999, non seulement je traiterai des activités de l'année écoulée, mais encore je passerai en revue l'évolution de la fonction d'examen du CST depuis ma nomination en 1996.

Les connaissances et les enseignements que m'a apportés mon premier mandat contribueront à assurer d'autres progrès pendant mon deuxième mandat, que le ministre de la Défense nationale a annoncé le 15 juin 1999. Ce nouveau mandat, qui sera en vigueur jusqu'au 19 juin 2002, reconduit

TABLE DES MATIÈRES

1	Trois années d'examen du CST
2	• Coup d'œil rétrospectif sur le premier mandat.....
4	• Technologie, protection de la vie privée et examen
5	• L'effet de l'examen sur le CST
6	Activités de l'année 1998-1999.....
6	• Vérification
8	• La fonction relative aux plaintes
10	• Autres activités.....
11	• Budget et personnel.....
12	Constatations faites en 1998-1999
12	Réexamen de la politique opérationnelle
13	La fonction d'examen.....
15	Adieu
17	Annexe A : Décret C.P. 1996-899
19	Annexe B : Etat des dépenses.....

Commissionnaire du Centre de la
sécurité des télécommunications

L'honorable Claude Bisson, O.C.



Communications Security
Establishment Commissioner

The Honourable Claude Bisson, O.C.

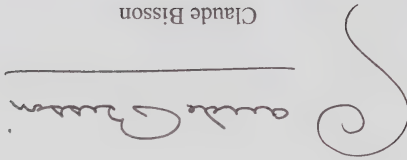
Juillet 1999

L'honorable Arthur C. Eggleton, C.P.,
Ministre de la Défense nationale
Édifice Mgén G.R. Pearkes, 13^e étage
101, promenade Colonel By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément à l'alinéa b) du décret C.P. 1996-899 prévoyant ma
nomination au poste de commissaire du Centre de la sécurité des télécommunica-
tions, j'ai le plaisir de vous soumettre mon troisième rapport annuel, qui fait état
de mes activités et constatations durant la dernière année de mon mandat, pour
présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma
haute considération.


Claude Bisson

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

Bureau du Commissaire du Centre de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044
Téléc. : (613) 992-4096

© Ministre des Travaux publics et des Services gouvernementaux Canada 1999
ISSN 1206-7490
N° de cat. D95-1999



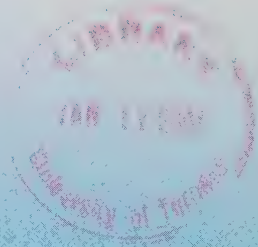
RAPPORT ANNUEL
du Commissaire du Centre de la sécurité
des télécommunications



Communications
Security
Establishment
Commissioner

Annual
Report

CA1
ND 800
-S16



1999
↓
2000

Canada

Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station 'B'
Ottawa, Ontario
K1P 5R5

Tel: (613) 992-3044
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 2000
ISSN 1206-7490
Cat. No. D95-2000

Communications Security
Establishment Commissioner



The Honourable Claude Bisson, O.C.

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Claude Bisson, O.C.

May 2000

The Honourable Arthur C. Eggleton, P.C.
Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Mr. Eggleton:

Pursuant to paragraph (g) of Order in Council P.C. 1999-1048 re-appointing me Communications Security Establishment Commissioner, I am pleased to submit to you my 1999-2000 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

A handwritten signature in black ink that reads "Claude Bisson". The signature is written in a cursive style. Below the signature is a horizontal line.

Claude Bisson

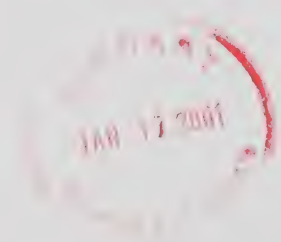


TABLE OF CONTENTS

A New Mandate.....	1
1999-2000 Review Undertakings	2
• Internal Investigations and Complaints	2
• Foreign Signals Intelligence	2
The Intelligence Cycle	3
‘Second Party’ Collection.....	5
• Information Technology Security	6
Budget and Staff.....	7
1999-2000 Findings.....	8
The Complaints Function	9
• Anonymous Allegations	9
Building Relationships	10
• DND Ombudsman.....	10
• International Conference	11
The Future of Review for CSE.....	12
My New Website	13
People and Places	13
Annex: Order in Council P.C. 1999-1048	15

A New Mandate

For the past four years I have had the responsibility of reviewing the activities of the Communications Security Establishment (CSE) and reporting to the Minister of National Defence on the lawfulness of those activities.

My initial three-year mandate was set out in a 1996 Order in Council of the Government of Canada under the *Inquiries Act*. On June 15, 1999, the Minister of National Defence announced that the government had renewed my appointment for another three years and enhanced my mandate by increasing my authority to respond to complaints about CSE. A copy of the new Order in Council appears as Annex A of this report.

This Annual Report – my fourth – covers the first year of my second mandate, up to the government's fiscal year end of March 31, 2000.

The task of reviewing CSE is an important and necessary one in a democratic society. An agency of Canada's Department of National Defence, CSE provides the Government of Canada with foreign signals intelligence (SIGINT), which it obtains by gathering and analyzing foreign radio, radar and other electronic emissions. Through its Information Technology Security program, CSE also provides advice on the security of the government's information technology.

To fulfil its mandate, CSE has, over the more than five decades of its existence, developed highly sophisticated technological capabilities. One of my functions is to review CSE's activities to ensure that the organization does not use its capabilities in ways that contravene the laws of Canada.

1999-2000 Review Undertakings

During this past year, I submitted four classified reports to the Minister of National Defence. One of these reports revisited the subject of internal investigations and complaints. The remaining reports presented the results of reviews of CSE activities related to its foreign signals intelligence and information technology security mandates. All studies included an examination of the legal parameters within which CSE operates, related policies and practices, and the accountability systems and procedures in place at CSE. None revealed issues of unlawful activity.

Internal Investigations and Complaints

When I first reviewed CSE's internal investigations and complaints in 1997-98, I observed that most dealt with such issues as security infractions, and none involved unlawful activity in the delivery of CSE's mandate. This was again the case this past year. In the interim, CSE implemented many new internal security policies and initiatives to heighten security awareness. These appear to have proven effective, in that there were far fewer incidents leading to internal investigations this past year than in 1997-98.

Foreign Signals Intelligence

In reviewing CSE's signals intelligence activities this past year, I noted a continuing enhancement and updating of SIGINT policies and directives in response to the evolving communications environment. I also observed new initiatives introduced by CSE to enhance its ability to manage and account for its SIGINT-related activities.

I paid particular attention this year to examining not only *what* CSE collects and retains, but *how* CSE's intelligence holdings are generated. As a result, I was able to further my knowledge and understanding of some of the highly specialized and technical means used to minimize the likelihood that private Canadian communications would make their way into CSE's

holdings. I am able to state that, as of this date, I am satisfied that, within the current technical environment, CSE is employing appropriate measures to safeguard the privacy of Canadians.

The Intelligence Cycle

In last year's report, I observed that CSE's activities are driven by its mandate to fulfil the foreign intelligence requirements established by the Government of Canada, not by the capabilities of the technology at hand.

Those requirements, in the form of foreign intelligence priorities for Canada's intelligence community, are set annually by a group of Cabinet ministers whose responsibilities touch on the country's security within Canada and abroad. The establishment of the Government of Canada's intelligence priorities is the first step in what the intelligence community calls the "intelligence cycle." It is worth examining that cycle briefly and looking at CSE's role in it.

The Government of Canada's foreign intelligence priorities form the basis of CSE's yearly SIGINT program. That is to say, these priorities are conveyed formally to CSE by the Deputy Secretary to the Cabinet, Security and Intelligence, Privy Council Office. CSE then uses these priorities to determine what information it seeks to obtain, either from its own activities or from the activities of its partner agencies in the United States, the United Kingdom, Australia, and New Zealand.

Concurrent with this, CSE must ensure that the appropriate steps are always taken to minimize the likelihood of intercepting the private communications of Canadians.

Next, CSE receives the inflow of intelligence traffic from multiple sources – its own and those of its partners. This traffic is then processed, analyzed

and assessed against the government's intelligence priorities. The resulting intelligence product is disseminated to the government departments responsible for protecting Canada's security, intelligence, economic and defence interests.

Intelligence dissemination is facilitated by knowledgeable CSE staff who provide a tailored and timely intelligence delivery service to some 800 senior decision makers in government on ongoing and emerging issues. This regular contact with the users of CSE's intelligence product ensures that requirements are updated and feedback is incorporated in the production process.

The intelligence cycle provides me with one framework for reviewing CSE's activities. I can examine the lawfulness of CSE's activities at each stage of the cycle. Through this work, I keep abreast of foreign intelligence collection capabilities and practices, signals processing, signals and intelligence analysis, and the dissemination of intelligence product to CSE's clients in government.

I believe the exploding yield of information carried by global communications networks increases the need to ensure that the privacy of Canadians is protected. I continue working to identify and understand the numerous technological initiatives that support intelligence gathering. I am also increasing my understanding of *how* some of these initiatives are applied. Within this intelligence cycle, however, my interest remains the identification and examination of any technical applications and initiatives CSE uses to *avoid*, or at least minimize, the likelihood of private Canadian communications making their way into CSE's holdings.

I am able to report that CSE has undertaken initiatives to advance its technological capability to ensure the protection of private Canadian communications. CSE is aware of both my interest in this area and the importance I attach to assessing compliance. I encourage CSE's research and development initiatives in this fast-paced technological environment.

'Second Party' Collection

As noted earlier, CSE receives signals intelligence gathered by other governments. CSE also contributes intelligence it collects to other governments. These partnership arrangements – with the United States, the United Kingdom, Australia, and New Zealand – were developed during the Second World War and maintained throughout the Cold War. Signals that are provided by one country to another are described as 'second party' collection.

The governments of the countries involved in this exchange of intelligence have policies to ensure the privacy of their citizens. In particular, each government has agreed not to undertake collection on behalf of a second party that would be illegal in the second party country. In other words, they do not do indirectly what they cannot do directly.

I have made a point of developing an understanding of these collaborative relationships, focusing not only on shared policies but also on actual practices. I have sampled the documentation and had access to some of the systems that support intelligence gathering and exchange. At this time I am satisfied that CSE is taking all reasonable steps to safeguard the privacy of Canadian communications.

Over the past four years, I have focused much of my effort on CSE's SIGINT activities. However, CSE has another important role in government – its Information Technology Security (ITS) mandate: CSE advises the government on how to maintain security in its use of information technology.

This year, my Office conducted an in-depth examination of the ITS program to determine whether its activities were lawful. The study involved, first, a review of CSE's ITS authorities and mandate as provided in direction given to the Chief, CSE. This was followed by an examination of the management control framework established to govern the conduct and performance of ITS activities. Step three was an analysis of the environmental factors and changing circumstances affecting the government's security requirements. Finally, strategies, plans, operations and projects were reviewed against the template established by the preceding steps to identify issues or activities for further exploration.

No evidence of unlawful activity was found. However, the study did reveal several pertinent facts:

- The trend in government and the private sector toward increased electronic business and service delivery is radically transforming the ITS program. Whereas previously the program's focus was the protection of classified information about a small number of government clients, now it is called upon increasingly to advise on protecting unclassified but sensitive information, including the electronic business transactions that underpin many government programs and operations.
- If Canadians are to have confidence in electronic commerce and the infrastructure that makes it possible, the government must have "made-in-Canada" solutions to security concerns. CSE is

well equipped to play a key role in this, but it must be given clear direction by government on this sensitive issue.

- For example, one effective means of confirming the security of information infrastructure is to attempt to penetrate the defences (e.g., to test so-called firewalls). This is called “ethical hacking.” CSE does not conduct such penetrations of active systems because this could reveal personal data, with privacy implications. However, the result is that mission-critical information technology systems are not tested for the full range of threat scenarios facing those systems.

Henceforth, I will closely monitor ITS involvement in these activities to ensure they comply with prevailing constraints. I also would encourage the government to give CSE clear policy direction regarding the role it should play in ensuring the security of Canada’s information infrastructure.

Budget and Staff

My annual budget allocation for the year 1999-2000 was augmented to \$635,500 to provide for additional expenses, including counsel, in support of my expanded complaints function. I can report that actual expenses incurred were within budget.

In addition to two full-time staff, I have continued the practice established during my first mandate of hiring subject matter experts under contract. At present, I have six contractors performing specialized work under this arrangement, all of whom have been security cleared for the purpose of their work.

As I have indicated in the past, I believe I have adequate financial and personnel resources to carry out the mandate I have been given.

1999-2000 Findings

Based on the results of our review and analysis, I am of the opinion that CSE has acted lawfully in the performance of its mandated activities for the period under review. I am also satisfied that CSE has not targeted the communications of Canadian citizens or permanent residents of Canada.

These findings are consistent with those from previous years, since the creation of this Office. Through the process of study and review, I am advancing my knowledge and understanding of how CSE conducts its mandated activities. As my depth of knowledge increases, so does the certainty of my approach to assessing the lawfulness of these activities. Of particular importance to me is the increasing confidence with which I can state my findings.

By their very nature, foreign intelligence activities raise questions, and sometimes concerns, on the part of the private citizen. And I can attest to the technical, legal and ethical complexity of the intelligence cycle. I believe, therefore, that the existence of my Office since 1996 has been a necessary and appropriate addition to Canada's intelligence community. It has been my experience that, since 1996, CSE's policies, procedures and, most important, its practices have reflected the presence of my Office and my review parameters as established by the Government of Canada.

This combination of advancing capabilities on the part of my Office and improved policies and practices on the part of CSE augurs well for the future. Nevertheless, I intend to remain vigilant in reviewing the activities of CSE, and I will ensure that our increasing abilities are applied robustly as I fulfil the responsibilities of this Office.

The Complaints Function

This was the first year in which I had the authority to respond directly to individuals who raise complaints about CSE's activities. Previously, under my original mandate, I could receive such complaints but I was not able to report to the complainants about my findings. I was pleased when this limitation was removed when my mandate was renewed.

To help members of the public understand the role of my Office, and in particular the complaints function, we published a brochure, *Safeguarding the Privacy of Canadians*. The brochure notes that because complaints may contain sensitive information or may affect the privacy of Canadians, my Office will accept complaints only by mail, addressed to me. Copies of the brochure are available upon request.

My background and training in arbitration and mediation before I became Commissioner have made me a strong advocate of the benefits of alternative dispute resolution. By bringing the two sides to a dispute together to seek a mutual solution, alternative dispute resolution can reduce both conflict and costs and lead to a settlement that leaves both sides satisfied. For this reason, I have incorporated alternative dispute resolution processes into the Office's mechanisms for addressing complaints.

During the past year, I responded to a number of enquiries from concerned individuals. I can report, however, that no formal complaints were received by my Office.

Anonymous Allegations

One option open to me in reviewing the activities of CSE is to guarantee anonymity to people, particularly current or former employees, who come to me with allegations of illegal activity by CSE. Some observers believe such an offer would enhance my ability to determine whether such activities were taking place.

I do not believe guaranteed anonymity for accusers is the right way to go. This approach would have the potential to poison the operating environment at CSE, or at any other institution with such a guarantee. Managers and co-workers could easily become reluctant to offer necessary criticisms and critiques of the work of other employees for fear that an offended employee could make anonymous unfounded accusations against them.

For these reasons, the complaints procedures I have established for this Office do not shield the identity of people who bring forth allegations of illegal activity by CSE. It is my belief that, by putting the appropriate mechanisms in place in an environment designed to address issues constructively, complainants will feel compelled to come forward, in good faith, to raise legitimate concerns. At the same time, I will not hesitate to use all the authority of my Office to ensure that complainants acting in good faith do not suffer reprisals from any quarter, regardless of the ultimate disposition of the issues they raise.

Building Relationships

The ability of my Office to review the activities of CSE can be enhanced by the relationships we have with stakeholders beyond CSE itself. During 1999-2000, two developments served to strengthen this Office's relationships with others.

DND Ombudsman

In June 1999, the Minister of National Defence announced the mandate of André Marin, the Ombudsman for the Department of National Defence (DND) and the Canadian Forces. The Ombudsman is designated to act on the Minister's behalf, independent of the chain of command, as a neutral and objective sounding board, mediator and reporter on matters related to the Department of National Defence and the Canadian Forces.

Because the Communications Security Establishment is an agency of DND, there is potential overlap between my role and that of the Ombudsman. In the autumn of 1999, Mr. Marin and I met to discuss our respective mandates as well as to establish clear boundaries and procedures for cooperation between our two Offices. We agreed the Ombudsman has an important role in addressing issues raised by CSE employees, but that role does not extend to activities related to the mandate of CSE. In other words, it is my responsibility to deal with issues involving CSE's SIGINT or ITS activities.

We are confident that, between the two of us, we can effectively and efficiently address any concerns that may arise about CSE.

International Conference

At the international level, the second conference of Inspectors-General and Review Agencies, which took place in Ottawa in June 1999, gave me an opportunity to discuss mutual interests with colleagues from Australia, New Zealand, the United Kingdom, the United States, Belgium and South Africa. The event was hosted by Canada's Security Intelligence Review Committee, the agency responsible for reviewing the Canadian Security Intelligence Service. The first such conference took place in Canberra, Australia in 1997.

Among the topics of discussion at the conference were relations between review organizations and legislators, and relationships with the media. The participation of Canadian parliamentarians and journalists made these sessions particularly informative. Equally valuable were the formal and informal exchanges with people from other countries who have responsibilities similar to my own. By comparing experiences, we learned how others have addressed the challenges we share.

The Future of Review for CSE

In prepared remarks to the conference of Inspectors-General and Review Agencies, I noted that over the past decade or two, many of our governments have increased their efforts to monitor and report on the lawfulness of their intelligence agencies – a trend I said was likely to continue. Government actions in this regard have been deliberate and carefully thought out, in keeping with the importance and sensitivity of intelligence activities, but the direction is clearly toward greater openness and increased accountability.

I noted that a key issue in the Canadian context is whether the Government of Canada should introduce legislation for CSE. I observed that any such legislation would likely include the creation of a permanent review mechanism in place of my fixed-term appointment by Order in Council.

As I have said before, I believe that legislation for CSE would be an appropriate development. However, if and when the government decides to move in this direction, it should act with the same caution and deliberation that have been the hallmarks of western governments in dealing with their intelligence agencies. In my view, the arrangements now in place to review CSE are entirely effective, and there is no urgency to alter them independent of the larger issue of whether CSE should have a legislative base. Permanent review arrangements should reflect the foreign intelligence nature of the work of CSE and the degree to which CSE could infringe on the rights and privacy of Canadians in fulfilling its mandate.

My New Website

Last year saw the launch of the official website of the Office of the Communications Security Establishment Commissioner. My objective with the site is to make information about this Office more readily available to the growing number of Canadians with access to the Internet. The site provides background on the mandate and functions of the Commissioner and access to my annual reports. The website address is <http://csec-ccst.gc.ca>.

People and Places

One of the challenges facing CSE in the past was that its employees were scattered in several buildings in Ottawa. That situation improved with the recent acquisition of the former Canadian Broadcasting Corporation headquarters, which is close to the main CSE facility, the Sir Leonard Tilley Building. The new building – now named the Edward Drake Building in honour of the first head of CSE's predecessor organization, the Communications Branch of the National Research Council – will allow CSE to consolidate most of its operations in the two buildings, under the leadership of its new Chief, Mr. D. Ian Glen.

On a separate note, the government and the people of Canada lost an outstanding public servant with the death in August 1999 of Mr. John Tait. I had the honour of knowing Mr. Tait when he was Deputy Minister of Justice and I was Chief Justice of Quebec. When I took on this job, he was the Coordinator of Security and Intelligence in the Privy Council Office and thereby the Deputy Minister responsible for CSE's policy and operations. Among his many other contributions to the government was a 1997 report on public service values and ethics, produced by a task force that he chaired. The document, now widely known as the Tait Report, has helped generate a strengthening of values-based governance in the Government of Canada.



CANADA

PRIVY COUNCIL • CONSEIL PRIVÉ

P.C. 1999-1048
June 8, 1999

His Excellency the Governor General in Council, on the recommendation of the Minister of National Defence, pursuant to Part II of the *Inquiries Act*, hereby authorizes the Minister of National Defence (in this order referred to as "the Minister")

(a) to re-appoint the Honourable Claude Bisson of Montreal, Quebec, for a period of three years, as a commissioner ("the Commissioner") to review the activities of the Communications Security Establishment ("CSE") for the purpose of determining whether those activities are in compliance with the law;

(b) to authorize the Commissioner to commence that review on his own initiative or at the request of the Minister;

(c) to authorize the Commissioner to investigate any complaint, concerning the lawfulness of CSE activities, made by any individual who is a Canadian citizen or a permanent resident of Canada;

(d) to authorize the Commissioner not to investigate complaints for which, in the Commissioner's opinion, other avenues of redress are established by statute;

(e) to specifically authorize the Commissioner to inform any complainant of the results of his investigation, ensuring that no classified information is disclosed to the complainant;

(f) to direct the Commissioner to inform the Minister and the Attorney General of Canada of any CSE activity that the Commissioner believes may not be in compliance with the law;

.../2

- 2 -

(g) to direct the Commissioner to submit to the Minister, once each year and in both official languages, a report on the Commissioner's activities and findings that are not classified, which report the Minister will table in Parliament;

(h) to authorize the Commissioner, at any time the Commissioner considers it advisable, to submit a report containing classified information to the Minister;

(i) to direct the Commissioner, before submitting any report to the Minister, to consult with the Deputy Secretary to the Cabinet (Security and Intelligence) at the Privy Council Office for the purpose of ensuring compliance with all security requirements and the preservation of the secrecy of sources of security and intelligence information and of the security of information provided to Canada in confidence by other nations;

(j) to direct the Commissioner and all persons engaged on his behalf take an oath of secrecy and comply with all applicable government security requirements;

(k) to authorize the Commissioner to engage the services of any staff, advisors and counsel that he considers necessary to assist him in the performance of his duties and functions at such rates of remuneration and reimbursement as may be approved by the Treasury Board;

.../3

- 3 -

(l) to fix the remuneration of the Commissioner at the per diem rate set out in the annexed schedule, which rate is within the range of \$400 to \$500; and

(m) to authorize that the Commissioner be paid reasonable travel and living expenses incurred by him in the performance of his duties and functions while absent from his ordinary place of residence, in accordance with Treasury Board travel directives;

effective June 19, 1999.

CERTIFIED TO BE A TRUE COPY-COPIE CERTIFIÉE CONFORME



CLERK OF THE PRIVY COUNCIL-LE GREFFIER DU CONSEIL PRIVÉ

1) à fixer la rémunération du commissaire au
taux journalier établi dans l'annexe
ci-jointe, lequel se situe entre 400 \$ et 500 \$;
m) à autoriser le remboursement des frais de
transport et de séjour raisonnables engagés
par le commissaire lorsque l'exercice de ses
fonctions l'amène à s'éloigner de son lieu de
résidence habituel, conformément aux
directives du Conseil du Trésor concernant
les déplacements;
à compter du 19 juin 1999.

CERTIFIED TO BE A TRUE COPY-COPIE CERTIFIÉE CONFORME



CLERK OF THE PRIVY COUNCIL-LE GREFFIER DU CONSEIL PRIVÉ

g) à enjoindre au commissaire de présenter au ministre, une fois l'an et dans les deux langues officielles, un rapport sur ses activités et ses constatations qui ne sont pas de nature confidentielle, le rapport devant être déposé par le ministre au Parlement;

h) à autoriser le commissaire à présenter au ministre, et ce à tout moment jugé opportun par le commissaire, un rapport contenant des renseignements confidentiels;

i) à enjoindre au commissaire, avant la présentation de tout rapport au ministre, de consulter le sous-secrétaire du Cabinet (Sécurité et renseignement) au Bureau du Conseil privé pour s'assurer que toutes les exigences relatives à la sécurité sont respectées, y compris la confidentialité des sources et la protection des renseignements obtenus de pays étrangers;

j) à exiger que le commissaire et toutes les personnes engagées pour son compte prononcent un serment de discrétion et se conforment à toutes les exigences du gouvernement en matière de sécurité;

k) à autoriser le commissaire à retenir les services de toute personne dont il juge avoir besoin pour l'assister dans ses fonctions, aux taux de rémunération et d'indemnisation que peut approuver le Conseil du Trésor;

.../3

f) à enjoindre au commissaire de signaler au ministre et au procureur général du Canada toute activité du CST qu'il estime ne pas être conforme à la loi;

e) à autoriser expressément le commissaire à informer toute personne ayant déposé une plainte des résultats de l'enquête qui a été effectuée, en prenant soin de ne divulguer aucun renseignement confidentiel à cette personne;

d) à autoriser le commissaire à ne pas instruire une plainte lorsque, de l'avis de celui-ci, il existe d'autres recours légaux;

c) à autoriser le commissaire à instruire toute plainte concernant la légalité des activités du CST que pourrait déposer un citoyen canadien ou un résident permanent du Canada;

b) à autoriser le commissaire à entreprendre cet examen de sa propre initiative ou à la requête du ministre;

a) à reconduire l'honorable Claude Bisson, de Montréal (Québec), dans ses fonctions de commissaire du Centre de la sécurité des télécommunications (le « CST ») pour une période de trois ans pendant laquelle il examinera les activités du CST et s'assurera qu'elles sont conformes à la loi;

Le « ministre » :

conseil autorise le ministre de la Défense nationale enquêtes, Son Excellence le Gouverneur général en nationale et en vertu de la partie II de la Loi sur les Sur recommandation du ministre de la Défense



Le site Web officiel du Bureau du commissaire du Centre de la sécurité des télécommunications est entré en service au cours de l'année dernière. Mon objectif, en établissant ce site, est de permettre au nombre croissant de Canadiens qui ont accès à Internet d'obtenir plus facilement de l'information au sujet de mon bureau. On y trouve des renseignements de base sur le mandat et les fonctions du commissaire, ainsi que mes rapports annuels. L'adresse en est la suivante : <http://csec-ccst.gc.ca>.

L'un des problèmes auxquels le CST a fait face par le passé a été l'éparpillement de ses employés dans plusieurs édifices à Ottawa. L'achat récent de l'ancien siège de la Société Radio-Canada, qui se trouve à proximité de l'édifice Sir Leonard Tilley, principale installation du CST, a amélioré cette situation. Le nouvel immeuble — maintenant baptisé édifice Edward Drake en l'honneur du premier dirigeant de l'ancêtre du CST, la Direction des communications du Conseil national de recherches — permettra à l'organisme de regrouper la plupart de ses activités dans les deux édifices, sous la direction de son nouveau chef, M. D. Ian Glen.

Dans un autre ordre d'idées, le gouvernement et la population du Canada ont perdu un fonctionnaire éminent lors du décès de M. John Tait, en août 1999. J'ai eu l'honneur de faire la connaissance de M. Tait lorsqu'il était sous-ministre de la Justice et que j'occupais la charge de juge en chef du Québec. Lorsque j'ai pris mes fonctions actuelles, il était coordonnateur de la sécurité et du renseignement au Bureau du Conseil privé et, de ce fait, sous-ministre responsable de la politique et des activités du CST. L'une de ses nombreuses contributions à l'administration fédérale a été un rapport sur les valeurs et l'éthique de la fonction publique, produit et publié en 1997 par un groupe de travail qu'il avait présidé. Ce document, maintenant appelé communément rapport Tait, a contribué à renforcer la gestion des affaires publiques fondée sur des valeurs au sein du gouvernement du Canada.

L'avenir de l'examen pour le CST

Dans une allocution rédigée en vue de la conférence des inspecteurs généraux et des organismes de surveillance, je mentionnais que, au cours des quelque 10 à 20 dernières années, nombre de nos gouvernements avaient intensifié leurs efforts de surveillance et de rapports touchant la légalité des activités de leurs services de renseignement, et je disais que cette tendance allait probablement se maintenir. Les mesures prises par les gouvernements à cet égard ont été mûrement réfléchies et conçues avec grand soin, compte tenu de l'importance et du caractère délicat des activités de renseignement, mais elles tendent manifestement vers une plus grande ouverture et une responsabilisation accrue.

J'ai signalé qu'une des questions clés qui se posent dans le contexte canadien consiste à savoir si le gouvernement du Canada devrait adopter une loi pour régir l'activité du CST. J'ai fait remarquer que, le cas échéant, cette loi prévoirait probablement la création d'un mécanisme d'examen permanent qui remplacerait ma nomination par décret pour une durée déterminée.

Comme je l'ai déjà dit, je pense qu'il serait opportun d'établir une loi visant le CST. Toutefois, si jamais le gouvernement décide d'agir dans ce sens, il devrait procéder avec la même prudence et la même réflexion que celle avec laquelle les gouvernements occidentaux ont abordé la surveillance de leurs services de renseignement. À mon avis, le mécanisme actuellement en place pour examiner les activités du CST est tout à fait efficace, et il n'y a aucune urgence à le modifier hors du contexte plus large de l'adoption éventuelle d'une loi visant cet organisme. Tout mécanisme d'examen permanent devrait tenir compte du fait que les travaux du CST ont trait aux renseignements sur l'étranger et de la mesure dans laquelle l'organisme pourrait porter atteinte aux droits et à la vie privée des Canadiens dans l'exécution de son mandat.

Conférence internationale

un rôle important à jouer pour résoudre les questions soulevées par des employés du CST, mais que ce rôle ne s'étend pas aux activités liées au mandat de l'organisme. Autrement dit, c'est à moi qu'il appartient de traiter les questions se rapportant aux activités du CST en matière de SIGINT et de STL. Nous sommes persuadés de pouvoir, de part et d'autre, résoudre réellement et efficacement toute préoccupation pouvant être soulevée au sujet du CST.

Au palier international, la deuxième conférence des inspecteurs généraux et des organismes de surveillance, qui s'est tenue à Ottawa en juin 1999, m'a fourni l'occasion de discuter de questions d'intérêt mutuel avec des collègues de l'Australie, de la Nouvelle-Zélande, du Royaume-Uni, des États-Unis, de la Belgique et de l'Afrique du Sud. Le Comité de surveillance des activités du renseignement de sécurité du Canada, qui est chargé de surveiller le Service canadien du renseignement de sécurité, en était l'hôte. La première de ces conférences avait eu lieu à Canberra (Australie) en 1997.

Citons parmi les sujets discutés à la conférence les relations entre les organismes de surveillance et les législateurs, et les relations avec les médias. La participation de parlementaires et de journalistes canadiens a fait que ces séances ont été particulièrement informatives. Les échanges de vues officiels et informels avec des gens d'autres pays qui ont des responsabilités semblables aux miennes ont également été précieux. En comparant nos expériences respectives, nous avons vu comment d'autres personnes ont relevé les mêmes défis que ceux auxquels nous sommes confrontés.

Développement de relations

Ombudsman du MDN

Pour ces raisons, la procédure de traitement des plaintes que j'ai établie pour mon bureau ne protège pas l'identité des personnes qui présentent des allégations d'activité illégale de la part du CST. J'estime que si l'on met en place les mécanismes appropriés dans un contexte conçu pour aborder les problèmes de manière constructive, les personnes qui ont des sujets de plainte légitimes se sentiront tenues de les présenter en toute bonne foi. Par ailleurs, je n'hésiterai pas à me servir de toute l'autorité attachée à mes fonctions pour m'assurer que les plaignants agissant de bonne foi ne subiront aucune mesure de représailles de quelque provenance que ce soit, indépendamment de la résolution finale des questions qu'ils auront soulevées.

Les relations qu'entretient mon bureau avec des parties intéressées au delà du CST lui-même peuvent accroître sa capacité d'examiner les activités de cet organisme. Au cours de l'année 1999-2000, deux facteurs ont permis de renforcer les relations de mon bureau avec d'autres parties.

En juin 1999, le ministre de la Défense nationale a rendu public le mandat de M. André Marin, ombudsman du ministère de la Défense nationale (MDN) et des Forces canadiennes. Celui-ci est désigné pour agir au nom du Ministre, indépendamment de la chaîne de commandement; il doit, de manière neutre et objective, formuler des avis, jouer un rôle de médiateur et faire rapport sur des questions se rapportant au ministère de la Défense nationale et aux Forces canadiennes.

Comme le Centre de la sécurité des télécommunications relève du MDN, il existe une possibilité de chevauchement entre mon rôle et celui de l'ombudsman. À l'automne de 1999, M. Marin et moi-même nous sommes réunis pour examiner nos mandats respectifs et pour établir des limites claires et des méthodes de coopération entre nos deux bureaux. Nous avons convenu que l'ombudsman a

Allegations anonymes

ou toucher la vie privée de Canadiens, mon bureau acceptera uniquement les plaintes qui me seront adressées personnellement par la poste. On peut obtenir des exemplaires de cette brochure sur demande.

Mes antécédents et ma formation dans le domaine de l'arbitrage et de la médiation avant ma nomination au poste de commissaire ont fait de moi un ardent avocat des avantages du règlement extrajudiciaire des différends. En amenant les deux parties à un différend à rechercher ensemble une solution mutuelle, cette formule peut réduire à la fois l'intensité des conflits et les coûts, et mener à un règlement satisfaisant pour l'une comme pour l'autre. C'est pourquoi j'ai intégré les procédés de règlement extrajudiciaire des différends aux mécanismes prévus par mon bureau pour résoudre les plaintes.

Au cours de l'année écoulée, j'ai répondu à un certain nombre de demandes de renseignements de citoyens inquiets. Je suis cependant à même de signaler que mon bureau n'a reçu aucune plainte officielle.

Dans l'examen des activités du CST, j'ai la possibilité de garantir l'anonymat aux personnes qui accusent l'organisme de se livrer à des activités illégales, en particulier s'il s'agit d'employés actuels ou d'ex-employés. De l'avis de certains observateurs, cela accroîtrait ma capacité de déterminer l'existence de telles activités.

Je ne pense pas que ce soit là une bonne façon de procéder. Le fait de garantir l'anonymat aux accusateurs pourrait empoisonner l'atmosphère de travail du CST, ou de toute autre institution qui offrirait une telle garantie. En effet, les gestionnaires et les collègues pourraient facilement en venir à hésiter à formuler des critiques ou des commentaires nécessaires au sujet du travail d'autres employés de crainte que ceux-ci s'offusquent et décident de porter contre eux des accusations anonymes sans fondement.

La fonction relative aux plaintes

connaissance, je suis de plus en plus sûr de ma méthode d'évaluation quant à la légalité de ces activités. L'assurance croissante avec laquelle je peux formuler mes constatations est particulièrement importante à mes yeux.

La nature même des activités de renseignement sur l'étranger soulève des questions, et parfois des préoccupations, chez les citoyens. Et je peux témoigner de la complexité du cycle du renseignement sur les plans technique, juridique et éthique. Je pense par conséquent que l'existence de mon bureau depuis 1996 a constitué un ajout nécessaire et opportun à la communauté canadienne du renseignement. J'ai constaté que, depuis 1996, les politiques et méthodes du CST et, par-dessus tout, ses pratiques reflètent la présence de mon bureau et mes paramètres d'examen tels qu'ils ont été établis par le gouvernement du Canada.

Les capacités croissantes de mon bureau, allées à l'amélioration des politiques et des pratiques du CST, sont de bon augure pour l'avenir. Néanmoins, j'entends rester vigilant dans l'examen des activités du CST, et je veillerai à ce que nous employions énergiquement ces capacités aussi longtemps que j'occuperai la charge de commissaire.

L'année écoulée a été la première au cours de laquelle j'ai eu le pouvoir de répondre directement aux personnes qui forment des plaintes au sujet des activités du CST. Auparavant, mon mandat initial me permettait de recevoir ces plaintes, mais non de faire rapport de mes constatations aux plaignants. J'ai été heureux de voir cette limite supprimée lors du renouvellement de mon mandat. Afin d'aider le grand public à comprendre le rôle de mon bureau et, en particulier, la fonction relative aux plaintes, nous avons publié une brochure intitulée *Protéger la vie privée des Canadiens*. On y signale que, comme les plaintes peuvent comporter des renseignements de nature délicate

J'encouragerais par ailleurs le gouvernement à donner des instructions claires au CST quant au rôle qu'il devrait jouer pour assurer la sécurité de l'infrastructure d'information du Canada.

Le budget qui m'avait été alloué pour l'année 1999-2000 a été porté à 635 500 \$ afin de couvrir des dépenses supplémentaires, dont des services de conseils juridiques, liées à l'expansion de mon mandat touchant les plaintes. Je suis à même de déclarer que les dépenses effectivement engagées ont respecté les limites de ce budget.

Conformément à la pratique établie au cours de mon premier mandat, j'ai continué à m'appuyer sur deux employées à plein temps et à retenir par contrat les services de spécialistes de questions particulières. À l'heure actuelle, six contractuels effectuent des travaux spécialisés selon cette formule, et tous possèdent l'autorisation de sécurité nécessaire à leur travail.

Comme je l'ai mentionné par le passé, j'estime disposer des ressources financières et en personnel voulues pour m'acquitter du mandat qui m'a été confié.

Budget et personnel

Constatations faites en 1999-2000

À la lumière des résultats de notre examen et de notre analyse, je suis d'avis que le CST s'est conformé à la loi dans l'exercice des activités prévues par son mandat au cours de la période examinée. Je suis par ailleurs convaincu qu'il n'a pas ciblé les communications de citoyens canadiens ni de résidents permanents du Canada. Ces constatations rejoignent celles que j'ai faites ces dernières années, depuis la création de mon bureau. Grâce à mon travail d'étude et d'examen, je connais et comprends de mieux en mieux la façon dont le CST exerce les activités prévues par son mandat. À mesure que j'approfondis cette

On n'a découvert aucune preuve d'activité illégale. Toutefois, cet examen a mis au jour plusieurs faits pertinents :

- La tendance de l'Administration et du secteur privé à recourir de plus en plus au commerce électronique et à fournir leurs services par voie électronique transforme radicalement le programme de STI. En effet, celui-ci était auparavant axé sur la protection des renseignements classifiés d'un petit nombre de clients de l'État, mais ses responsables sont de plus en plus appelés à donner des conseils sur la protection de renseignements non classifiés mais de nature délicate, dont les opérations de commerce électronique qui sous-tendent nombre de programmes et d'activités de l'État.
- Si le gouvernement veut que les Canadiens aient confiance dans le commerce électronique et l'infrastructure qui le rend possible, il doit pouvoir offrir des solutions « canadiennes » aux préoccupations relatives à la sécurité. Le CST possède les moyens voulus pour jouer un rôle clé à cet égard, mais il doit recevoir des instructions claires du gouvernement sur cette question délicate.

- Par exemple, un moyen efficace de vérifier la sécurité de l'infrastructure d'information consiste à essayer d'en pénétrer les barrières (autrement dit à en éprouver les « pare-feu »). On parle alors de « piraterie éthique ». Le CST ne pénétre pas de systèmes actifs de cette manière, car cela pourrait mettre au jour des données personnelles, ce qui aurait des répercussions sur la vie privée. Toutefois, cela a pour résultat que les systèmes de technologies de l'information essentiels ne sont pas vérifiés par rapport à la gamme complète des menaces auxquelles ils sont exposés.

Je surveillerai désormais de près la participation du programme de STI à ces activités pour m'assurer qu'elles respectent les limites actuelles.

Sécurité des technologies de l'information

En particulier, chaque gouvernement a convenu de ne pas effectuer, pour le compte d'une seconde partie, de travail de collecte qui serait illégal dans le pays de cette seconde partie. Autrement dit, ils ne font pas indirectement ce qu'ils ne peuvent pas faire directement.

Je me suis fait un devoir de me familiariser avec ces rapports de collaboration en étudiant non seulement les politiques communes, mais encore les pratiques. J'ai procédé à un échantillonnage de la documentation et j'ai eu accès à certains des systèmes qui appuient la collecte et l'échange de renseignements. J'ai actuellement la conviction que le CST prend toutes les mesures raisonnables pour sauvegarder le caractère privé des communications des Canadiens.

Au cours des quatre dernières années, j'ai concentré une bonne partie de mon travail sur les activités de SIGINT du CST. Toutefois, celui-ci joue un autre rôle important au sein de l'administration fédérale. Dans le cadre de son mandat touchant la sécurité des technologies de l'information (STI), le CST donne en effet des conseils au gouvernement sur la façon de préserver la sécurité lorsqu'il a recours à ces technologies.

Cette année, mon bureau a procédé à un examen en profondeur du programme de STI afin de déterminer si ses activités étaient légales. On a d'abord examiné les pouvoirs et le mandat du CST en matière de STI, tels qu'ils sont prévus dans les directives données au chef du CST. On a ensuite examiné le cadre de contrôle de la gestion établi pour régir la conduite et l'exécution des activités de STI. On a analysé en troisième lieu les facteurs liés au contexte et les circonstances nouvelles qui influent sur les besoins du gouvernement en matière de sécurité. On a enfin examiné les stratégies, les plans, les opérations et les projets en regard du modèle établi grâce aux étapes précédentes afin de cerner les questions ou activités à étudier plus avant.

Collecte de
renseignements
« par une seconde
partie »

J'estime que la profusion d'information transportée par les réseaux de communications mondiaux accroît la nécessité de veiller à protéger la vie privée des Canadiens. Je continue à travailler pour reconnaître et comprendre les nombreuses initiatives technologiques qui appuient la collecte de renseignements. J'approfondis en outre ma connaissance de la façon dont on applique certaines de ces initiatives. Toutefois, ce qui m'intéresse dans le cycle du renseignement, c'est la reconnaissance et l'examen de toutes les applications et initiatives techniques que le CST utilise pour éviter, ou à tout le moins réduire au minimum, la probabilité que des communications privées de Canadiens se retrouvent dans ses fonds de renseignements.

Je suis à même de déclarer que le CST a pris des initiatives pour perfectionner ses moyens techniques afin d'assurer la protection des communications privées des Canadiens. Le CST est au courant de l'intérêt que je porte à cette question et de l'importance que j'attache à l'évaluation de sa conformité à cet égard. J'encourage les initiatives de recherche et de développement du CST dans notre contexte technologique en évolution rapide.

Comme je l'ai mentionné plus haut, le CST reçoit des renseignements électromagnétiques recueillis par d'autres gouvernements. Il fournit également à ceux-ci des renseignements qu'il a lui-même recueillis. Ces accords de partenariat avec les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande ont été établis au cours de la Deuxième Guerre mondiale et maintenus pendant toute la durée de la guerre froide. Lorsqu'un pays fournit ainsi des signaux à un autre pays, on parle de collecte de renseignements « par une seconde partie ».

Les gouvernements des pays qui participent à cet échange de renseignements ont des politiques destinées à protéger la vie privée de leurs citoyens.

renseignements il cherche à tirer de ses propres activités ou de celles de ses partenaires aux États-Unis, au Royaume-Uni, en Australie et en Nouvelle-Zélande.

Parallèlement, le CST doit s'assurer que l'on prend toujours les mesures voulues pour réduire au minimum la probabilité d'intercepter les communications privées de Canadiens.

Ensuite, le CST reçoit le flux de transmissions de nombreuses sources, tant les siennes propres que celles de ses partenaires. Ces transmissions sont ensuite traitées, analysées et évaluées par rapport aux priorités du gouvernement en matière de renseignement. Les renseignements qui en résultent sont diffusés aux ministères chargés de protéger les intérêts du Canada sur les plans de la sécurité, du renseignement, de l'économie et de la défense.

La diffusion des renseignements est facilitée par le personnel du CST, qui est bien informé et qui offre à quelque 800 décideurs de haut niveau de l'administration publique un service de prestation de renseignement adapté et opportun sur des questions nouvelles ou courantes. Ces contacts réguliers avec les utilisateurs de ses produits de renseignement permettent au Centre de mettre à jour les besoins et de prendre en compte les réactions des clients dans son processus de production.

Le cycle du renseignement me fournit un cadre pour examiner les activités du CST. Je peux vérifier la légalité de ces activités à chaque étape du cycle. Grâce à ce travail, je me tiens au courant des moyens et pratiques en matière de collecte de renseignements sur l'étranger, du traitement des signaux, de l'analyse des signaux et des renseignements, et de la diffusion des produits du renseignement aux clients du CST à l'administration fédérale.

Le cycle du renseignement

J'ai fait particulièrement attention, cette année, à examiner non seulement *la nature* des renseignements que le CST recueille et conserve, mais aussi *la façon* dont ses fonds de renseignements sont créés. Cela m'a permis de mieux connaître et comprendre certains des moyens très spécialisés et très techniques employés pour réduire au minimum la probabilité que des communications privées de Canadiens se retrouvent dans les fonds de renseignements du CST. Je suis en mesure d'affirmer qu'à ce jour, je suis convaincu que, dans le contexte technique actuel, le CST emploie des mesures appropriées pour protéger la vie privée des Canadiens.

Dans mon rapport de l'année dernière, je mentionnais que le moteur des activités du CST est son mandat de répondre aux besoins de renseignement sur l'étranger établis par le gouvernement du Canada, et non pas les capacités de la technologie dont il dispose.

Ces besoins, qui prennent la forme des priorités de la communauté canadienne du renseignement en matière de renseignement sur l'étranger, sont établis annuellement par un groupe de ministres du Cabinet, dont les responsabilités touchent à la sécurité intérieure et extérieure du Canada. La définition des priorités du gouvernement du Canada est la première étape de ce que la communauté du renseignement est convenue d'appeler le « cycle du renseignement ». Il vaut la peine d'examiner brièvement ce cycle et le rôle qu'y joue le CST.

Les priorités du gouvernement du Canada en matière de renseignement sur l'étranger forment la base du programme annuel de SIGINT du CST. Ces priorités sont communiquées officiellement au CST par le sous-secrétaire du Cabinet (sécurité et renseignement), du Bureau du Conseil privé. Le CST les utilise ensuite pour déterminer quels

Travaux d'examen en 1999-2000

Enquêtes et plaintes internes

Au cours de l'année écoulée, j'ai présenté quatre rapports classifiés au ministre de la Défense nationale. L'un de ceux-ci réexaminait la question des enquêtes et des plaintes internes. Les trois autres présentaient les résultats d'examens d'activités menées par le CST en matière de renseignement sur l'étranger et de sécurité des technologies de l'information. Toutes ces études comportaient un examen des paramètres juridiques régissant les activités du CST, des politiques et pratiques connexes et des systèmes et mécanismes de responsabilisation en place au sein de l'organisme. Aucune n'a révélé de problème ayant trait à des activités illégales.

Lors de mon premier examen des enquêtes et des plaintes internes, en 1997-1998, j'ai constaté que la plupart avaient rapport à des questions comme les infractions à la sécurité et que, dans aucun cas, le CST ne s'était livré à des activités illégales dans l'exécution de son mandat. J'ai fait la même constatation cette année. Dans l'intervalle, le CST a mis en œuvre un bon nombre de nouvelles politiques et initiatives internes destinées à sensibiliser davantage le personnel à la sécurité. Ces mesures semblent avoir été efficaces, en ce sens que le nombre des incidents ayant nécessité des enquêtes internes a été beaucoup moins élevé au cours de l'année dernière qu'en 1997-1998.

Renseignements électromagnétiques sur l'étranger

Dans mon examen des activités du CST en matière de renseignement électromagnétique sur l'étranger au cours de l'année écoulée, j'ai remarqué que l'on améliorerait et révisait constamment les politiques et directives en la matière, compte tenu de l'évolution dans le domaine des communications. J'ai en outre relevé les nouvelles initiatives instaurées par le CST afin d'accroître sa capacité de gérer ses activités liées au SIGINT et de rendre compte de celles-ci.

J'ai, depuis quatre ans, la responsabilité d'examiner les activités du Centre de la sécurité des télécommunications (CST) et de faire rapport au ministre de la Défense nationale sur leur légalité. Mon premier mandat de trois ans était énoncé dans un décret pris par le gouvernement du Canada en 1996 en vertu de la *Loi sur les enquêtes*. Le 15 juin 1999, le ministre de la Défense nationale a annoncé que le gouvernement avait renouvelé mon mandat pour trois autres années et j'avais étendu en élargissant mon pouvoir de répondre aux plaintes au sujet du CST. Une copie du nouveau décret figure à l'annexe A du présent rapport.

Ce rapport annuel, qui est mon quatrième, couvre la première année de mon deuxième mandat, jusqu'à la fin de l'année financière du gouvernement, soit le 31 mars 2000.

Le travail d'examen des activités du CST est important et nécessaire dans une société démocratique. Le CST, qui est un organisme du ministère de la Défense nationale, fournit au gouvernement du Canada des renseignements électromagnétiques sur des pays étrangers (SIGINT) qu'il obtient en recueillant et en analysant leurs transmissions par radio, par radar et par d'autres moyens électroniques. Dans le cadre de son programme de sécurité des technologies de l'information, il donne en outre des conseils sur la sécurité des technologies de l'information du gouvernement.

Le CST existe depuis plus de 50 ans. Au cours de cette période, il a mis au point des moyens techniques très perfectionnés en vue d'exécuter son mandat. L'une de mes fonctions consiste à examiner ses activités afin de m'assurer qu'il n'emploie pas ces moyens de manière contraire aux lois du Canada.

TABLE DES MATIÈRES

1	Nouveau mandat.....
2	Travaux d'examen en 1999-2000.....
2	Enquêtes et plaintes internes.....
2	Renseignements électromagnétiques sur l'étranger.....
3	Le cycle du renseignement.....
5	Collecte de renseignements « par une seconde partie ».....
6	• Sécurité des technologies de l'information.....
8	Budget et personnel.....
8	Constatations faites en 1999-2000.....
9	La fonction relative aux plaintes.....
10	• Allégations anonymes.....
11	Développement de relations.....
11	• Ombudsman du MDN.....
12	• Conférence internationale.....
13	L'avvenir de l'examen pour le CST.....
14	Mon nouveau site Web.....
14	Personnel et locaux.....
15	Annexe : Décret C.P. 1999-1048.....

Communications Security
Establishment Commissioner



CANADA

The Honourable Claude Bisson, O.C.

Mai 2000

L'honorable Arthur C. Eggleton, C.P.
Ministre de la Défense nationale
Édifice Mgén G.R. Pearkes, 13^e étage
101, promenade Colonel By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément à l'alinéa g) du décret C.P. 1999-1048 prévoyant le renouvellement de ma nomination au poste de commissaire du Centre de la sécurité des télécommunications, j'ai le plaisir de vous soumettre mon rapport annuel pour l'année 1999-2000, qui fait état de mes activités et constatations, pour présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

A stylized, handwritten signature of Claude Bisson, consisting of a large, flowing 'S' shape followed by the name 'Claude Bisson' in a cursive script.

Claude Bisson

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

Bureau du Commissaire du Centre de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044

Télex. : (613) 992-4096

© Ministère des Travaux publics et des Services gouvernementaux Canada 2000
ISSN 1206-7490
N° de cat. D95-2000



1999
↑
2000

Rapport
annuel



Commissaire
du Centre
de la sécurité
des télécommunications

CA1
ND800
- S16

Annual Report

2000
↓
2001

Communications
Security
Establishment
Commissioner



Canada

Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station 'B'
Ottawa, Ontario
K1P 5R5

Tel: (613) 992-3044
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 2001
ISBN 0-662-65817-5
Cat. No. D95-2001

Communications Security
Establishment Commissioner



The Honourable Claude Bisson, O.C.

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Claude Bisson, O.C.

May 2001

The Honourable Arthur C. Eggleton, P.C.
Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Mr. Eggleton:

Pursuant to paragraph (g) of Order in Council P.C. 1999-1048 re-appointing me Communications Security Establishment Commissioner, I am pleased to submit to you my 2000-2001 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Claude Bisson



TABLE OF CONTENTS

Introduction	1
CSE Today	2
• Mandate	2
• Signals Intelligence.....	2
• Information Technology Security	3
• Relationships with allies	4
• Controls on CSE's activities	4
• CSE's recent contributions	5
Evolution of CSE	6
• The pressures for change	6
• CSE's strategic plan	7
Reviewing CSE	8
• The Commissioner's role	8
• 2000-2001 activities.....	9
• Foreign intelligence product	9
• Information management.....	10
• Policy authority	11
• Other activities	11
• 2000-2001 findings.....	12
• Office staff and budget	12
Looking Ahead	13
• Safeguarding the privacy of Canadians	13
Annex A: Commissioner's Mandate	15
Annex B: Classified Reports, 1996-2001	19

INTRODUCTION

In the five-year period since my appointment, I have observed the emergence of complex global communications technologies, together with evolving political, social and economic realities. This environment has led to the identification of new threats to Canada's security, defence and national interests and a pressing need for the Government of Canada to determine how to counter these threats.

During this same period, the Communications Security Establishment (CSE) has sought to maintain its ability to meet the government's evolving foreign intelligence priorities and to protect the integrity of its communications and information systems.

I believe that a failure to maintain CSE's capabilities would have serious implications for Canada's national interests. For example, if CSE were unable to report on the activities and intentions of foreign states and persons, Canada's political and economic well-being would be at risk. Furthermore, if CSE could no longer protect government information systems and assets, the government's efforts would be crippled in the areas of electronic service delivery and e-commerce, ultimately to the detriment of Canada's economic competitiveness.

Technological advancements will certainly continue and may even accelerate. CSE's senior management has informed me that they are convinced CSE must refocus its efforts to meet its responsibilities to government, or risk lagging behind. As a result, in consultation with its stakeholders, CSE has adopted a renewed strategic approach to its mandate.

This is the environment in which I continue to examine CSE's activities to determine their compliance with the laws of Canada and to assess CSE's efforts to safeguard the privacy of Canadians.

As in my previous annual reports, I will look back in this 2000-2001 Annual Report on CSE's performance over the past year.

CSE TODAY

Mandate

CSE, an agency of the Department of National Defence, assists the Government of Canada in two distinct but related areas:

- It provides the government with foreign intelligence by collecting, analyzing and reporting on foreign radio, radar and other electronic signals (signals intelligence, or SIGINT).
- It helps ensure the Canadian government's telecommunications and information technologies are secure from interception, disruption, manipulation or sabotage (information technology security, or ITS).

The Minister of National Defence is fully accountable to Parliament for CSE. He is supported by two senior officials — the Deputy Minister of National Defence, for financial and administrative matters, and the Deputy Clerk of the Privy Council, Counsel and Security and Intelligence Coordinator, for policy and operational matters.

Signals Intelligence

CSE's SIGINT program is guided by the foreign intelligence priorities established annually by the Meeting of Ministers on Security and Intelligence, chaired by the Prime Minister.

To fulfill its SIGINT mandate, CSE acquires various modes of foreign communications signals. The collection and processing of these signals involve highly sophisticated and complex technologies. Processing often includes the decryption and translation of encrypted communications to make them intelligible.

Encryption falls within the science known as cryptology, which uses mathematical algorithms to hide or disguise communications.

I have learned from CSE that advancements in global transmissions present continuing challenges to the collection and processing of foreign signals. The tremendous volume of communications signals produced every day, together with the increased use and public availability of encryption software, has added to these challenges.

As a result, CSE has dedicated additional resources to the research and development of techniques to acquire and process communications, so that the government can be kept apprised of threats to Canada's interests. To accomplish this, CSE relies on the capabilities of a cross-section of skilled workers, including computer scientists, mathematicians and linguists. To produce intelligence reports it also needs analysts knowledgeable in such matters as international political, economic and military affairs, terrorism, and transnational crime. These reports are the vehicle through which CSE communicates foreign intelligence information to its Government of Canada clients. More than 100,000 SIGINT reports are made available to CSE's readership every year.

Information Technology Security

The development and application of new technologies in recent years has transformed the focus and complexity of the activities undertaken by CSE to protect government communications and communications systems, the mandate of its Information Security Technology (ITS) program.

Until fairly recently, computer hardware, software and networks were not widely available and had limited application. Today, however, the computer is a fully established means of daily

communication among people. It drives many of the technologies that make up Canada's critical information infrastructure.

This communications environment has introduced new vulnerabilities to government information systems that require alternative solutions to counter threats to security and privacy.

The government looks to CSE to protect information stored or transmitted on its computer systems while, at the same time, departments and agencies work toward making a multiplicity of services available to the public on-line. Meanwhile, by law, personal information about Canadians must be protected, despite the fact that government computer systems are increasingly interconnected and vulnerable to disruption and to such threats as denials of service.

Relationships with allies

Canada benefits from longstanding arrangements between CSE and its counterparts in the United States, the United Kingdom, Australia, and New Zealand. These arrangements, which were formalized after the Second World War and maintained during the Cold War, allow for the exchange of signals intelligence, technology and information about sources and techniques of shared interest.

As part of my ongoing review of CSE's activities, I am satisfied that CSE does not use its partners to circumvent the laws of Canada, nor does it provide partners with communications they could not legally collect for themselves.

Controls on CSE's activities

Based upon my review activities to date, I have observed that CSE's activities are guided by law and policy and the government's priorities, not by its technical capabilities. In addition to my own reviews, CSE is also subject to the independent

scrutiny of many, including the courts, the Privacy Commissioner, the Information Commissioner, the Canadian Human Rights Commission, and the Auditor General of Canada.

Today's global communications networks generate an inordinate volume of information with which CSE must contend. This volume is in and of itself a control. In practical terms, CSE must stay focused on its mandate in order to meet the foreign intelligence priorities it is given.

CSE's recent contributions

The government uses CSE's intelligence reporting to further Canada's economic and political interests in its relationships with foreign states.

The Canadian Forces enter peacekeeping operations abroad with an enhanced understanding of the situation on the ground as a result of CSE's contributions.

CSE provides its government clients responsible for protecting public safety with information derived from foreign intelligence that contributes to efforts directed at countering terrorism, weapons proliferation, drug smuggling, illegal migration, and transnational crime. More recently, CSE has begun to provide these same clients with technical assistance.

CSE is working closely with the Canadian Forces Information Operations Group (CFIOG) to enhance support to Canadian military operations, with direct service now provided by CFIOG. (CFIOG was created in April 1998 from a consolidation of various National Defence elements, including the Canadian Forces Supplementary Radio Systems. It provides a focal point for Information Operations).

Through its ITS program, CSE continues to encourage and support Canadian firms in the development of new security products.

Additionally, CSE has an ongoing relationship with several government departments and agencies and assists them in assessing their ITS needs as they migrate toward on-line service delivery.

CSE provided senior level expertise to the government's Critical Infrastructure Protection Task Force. Created in April 2000, the Task Force recommended what the federal government should do to protect that part of Canada's infrastructure that is critical to the health, safety, security, and economic well-being of Canadians.

EVOLUTION OF CSE

The pressures for change

CSE must contend with the revolutionary pace of technological change. The foundation of its activities is technology, which affects CSE, like its partners, in several ways:

- The channels through which foreign communications travel are multiplying. The new wireless, fibre optic and Internet communications technologies continue to advance, requiring CSE's computer scientists and engineers to expand and upgrade their knowledge base constantly.
- The targets of foreign intelligence collection activities, including terrorist groups, now have easy access to the sophisticated products of a multi-trillion dollar telecommunications industry, including digital encryption technology, available as freeware on the World Wide Web, making it difficult if not impossible to decipher their communications.
- Increasingly, vast amounts of information are moving through new channels of communication, making it highly labour-intensive for CSE to identify useful information.
- Canadian government departments and agencies are also using new modes of communication that interconnect with computer systems that contain

sensitive information or control critical infrastructure. They look to CSE's ITS experts for advice to protect their communications networks and computer systems.

- The number of attacks on government networks and systems is growing. A September 2000 study on threats to federal Internet sites estimated that a typical site is subject to 10 or more threat incidents each week. Moreover, the frequency of foreign attacks on US systems that originate or pass through Canada is becoming an issue.
- The government's new Office of Critical Infrastructure Protection and Emergency Preparedness, announced in February 2001 and charged with developing and implementing a comprehensive approach to protecting Canada's critical infrastructure, will look to CSE for technical support.

CSE's strategic plan

During the year under review, CSE embarked upon an important strategic exercise to identify alternative approaches to delivering its mandate.

As a starting point, CSE defined its vision: "to be the agency that masters the global information network to enhance Canada's safety and prosperity". In so doing, CSE has effectively returned to its roots with the recognition that its core strength is its ability to understand and protect communications and communications systems. CSE's ability to exploit these systems to provide foreign intelligence flows from this core strength.

In support of its vision, CSE aims to become a centre of excellence that develops and applies its technical expertise and understanding of global communications networks and helps Canada meet its critical information needs.

CSE has adopted three strategic goals for the next 10 years:

- to be the acknowledged governmental centre of excellence in understanding and addressing the capacities of the global network
- to protect and enable the Canadian information infrastructure
- to modernize CSE services, products and delivery.

As a first step, CSE has strengthened the linkage between its SIGINT and ITS programs. Although their activities are related, they have traditionally operated at arm's length from each other. To achieve its strategic goals, CSE intends to benefit from the synergies created by drawing the two programs closer. By exploring the vulnerabilities of communications and information systems together, SIGINT and ITS experts now pool their knowledge to identify threats to Canadian systems as well as opportunities for foreign intelligence collection.

In June 2000, the Chief of CSE briefed me on this topic. Subsequently, my office has discussed the strategy in detail with CSE's senior management. I do not believe this approach will change how I review CSE's activities in any fundamental way, since my focus will remain on their lawfulness. In the meantime, I have expressed my support of this undertaking.

REVIEWING CSE

The Commissioner's role

My mandate to review the activities of CSE and to report to the Minister of National Defence is contained in an Order in Council (see Annex A).

Each year, my office identifies areas within CSE's operations where, at first view, questions of lawfulness might be presumed. Under my authority, my office then conducts systematic reviews of these

operations. I pass the results of these reviews to the Minister of National Defence in the form of classified reports. The fact that I have issued a classified report is not an indication that I have uncovered an incident of unlawfulness. Rather, it is an indication that the report contains sensitive information that requires classified handling.

The effort that goes into researching and preparing my reports to the Minister accounts for the bulk of the work of my office and gives me a detailed understanding of various aspects of CSE's operations.

I have reviewed CSE's authorities to collect foreign intelligence on behalf of the Government of Canada and its mandate to protect the security of the government's information technology. On an ongoing basis, I examine CSE's policies, directives and actual practices to ensure they contribute to lawfulness and to protecting Canadians' privacy.

Among other issues, my reviews have looked at how CSE provides intelligence reports to its clients, and the receipt of intelligence from its Second Party partners. I regularly monitor CSE's operational activities, as well as circumstances that have led to internal security investigations.

Annex B contains a list of the classified reports I have passed to the Minister since my appointment in 1996.

2000-2001 activities

Foreign intelligence product

During the past year, I continued to review CSE's activities as they relate to the intelligence cycle and the handling and production of intelligence product. As I outlined in my last annual report, CSE conducts daily reviews of the raw traffic it receives from multiple sources and assesses its foreign intelligence value against the government's

priorities. CSE then passes the results to its government clients in the form of intelligence product.

This past year, I reviewed the policies and handling practices associated with CSE's receipt and retention of foreign intelligence traffic. I examined how CSE identifies issues of intelligence interest within the raw traffic it receives and the practices associated with its retention and subsequent dissemination in the form of intelligence reporting. And, as is my practice, I reviewed CSE's policies and practices, within this cycle of activities, that deal specifically with safeguarding the privacy of Canadians.

Information management

I also reviewed CSE's information management policies in light of the National Archives of Canada Act and Treasury Board policy and guidelines related to the management of information holdings.

Government departments and agencies are required to establish Records Disposition Authorities for their operational and administrative holdings. These Authorities grant permission to departments and agencies to dispose of certain holdings and require them to forward to the National Archives other holdings identified to be of archival interest, for preservation.

I observed that these Authorities do not constitute a requirement to destroy records, nor do they provide direction regarding the timing of records destruction. Moreover, they do not provide or authorize records retention periods. Retention and disposal periods are determined by the designated Minister of the institution and must, of course, conform to any other applicable legislation.

I was satisfied that CSE's policies conform with existing law and policy requirements related to the management of government information holdings. I recommended, however, that CSE give priority to completing its retention and disposal schedules.

Policy authority

In my 1998-99 Annual Report, I indicated my intention to examine the new framework for policy authority, accountability and coordination that CSE had recently adopted. Of particular interest to me were two of the objectives of the framework: to identify the appropriate level of authority for various policies; and to provide a desirable level of operational flexibility in support of day-to-day activities.

During the past year, I reviewed the new framework and found it to be well conceived and sound. It will take time, however, to convert all CSE policy to the framework. While some policy gaps remain, CSE has policies for its major requirements, and the new system should address my earlier concerns about having policy in the right place and signed off at the right level.

During the year under review, I was pleased to learn that officials had opened discussions on having cornerstone internal policies issued to CSE as Ministerial direction. I applaud this initiative, because it will strengthen the accountability linkages between CSE and the Minister of National Defence, who is responsible for CSE in Parliament.

Other activities

My mandate authorizes me to investigate complaints by Canadians or permanent residents of Canada about CSE activities. While there were informal inquiries during 2000-2001, none led to a formal complaint.

During the past year, my office has maintained its informal contacts within the security and intelligence community. We were particularly pleased to receive the Inspector General of South Africa during his autumn 2000 tour of North America. I look forward to renewing acquaintances with my counterparts from other countries at the upcoming conference of review agencies in Washington in October 2001.

2000-2001 findings

I am satisfied that during the period under review, CSE acted lawfully in the performance of its mandated activities and did not target the communications of Canadian citizens or permanent residents. I make this statement on the basis of the thorough review of CSE's activities conducted during the year.

My mandate requires me to inform the Minister of National Defence and the Attorney General of Canada of any CSE activity that I believe may not be in compliance with the law. To date, I have not been required to do so. CSE is aware of its boundaries, receives legal advice from counsel appointed to CSE by the Department of Justice, and has policies and procedures in place to promote lawfulness. These measures have proven to be effective.

Office staff and budget

During the 2000-2001 fiscal year, my budget allocation was \$648,800. I can report that actual expenses incurred were well within budget.

My office continues to consist of two full-time employees and a number of subject-matter experts whom I employ on contract. At present, there are five people performing specialized work under this arrangement, all of whom have the required security clearances. This provides me with both continuity and flexibility to obtain the expertise I require to review CSE's activities effectively.

LOOKING AHEAD

Safeguarding the privacy of Canadians

As I have previously observed, CSE's foreign intelligence collection technology must constantly progress to keep pace with advances in communications technology. Despite the efficiencies inherent in new technologies, CSE is still likely to receive inadvertently some small amount of Canadian communications. Moreover, each new collection system or technique that comes on stream seems to bring with it this potential. However, CSE is well aware that it must continually upgrade its capabilities to screen out Canadian communications or risk acting unlawfully if it does not make every effort to do so.

In this regard, I have informed CSE that, in addition to my other review activities, I will be seeking assurance that it is availing itself of all emerging technologies to ensure that the privacy of Canadians is safeguarded.



CANADA

PRIVY COUNCIL • CONSEIL PRIVÉ

P.C. 1999-1048

June 8, 1999

His Excellency the Governor General in Council, on the recommendation of the Minister of National Defence, pursuant to Part II of the *Inquiries Act*, hereby authorizes the Minister of National Defence (in this order referred to as "the Minister")

(a) to re-appoint the Honourable Claude Bisson of Montreal, Quebec, for a period of three years, as a commissioner ("the Commissioner") to review the activities of the Communications Security Establishment ("CSE") for the purpose of determining whether those activities are in compliance with the law;

(b) to authorize the Commissioner to commence that review on his own initiative or at the request of the Minister;

(c) to authorize the Commissioner to investigate any complaint, concerning the lawfulness of CSE activities, made by any individual who is a Canadian citizen or a permanent resident of Canada;

(d) to authorize the Commissioner not to investigate complaints for which, in the Commissioner's opinion, other avenues of redress are established by statute;

(e) to specifically authorize the Commissioner to inform any complainant of the results of his investigation, ensuring that no classified information is disclosed to the complainant;

(f) to direct the Commissioner to inform the Minister and the Attorney General of Canada of any CSE activity that the Commissioner believes may not be in compliance with the law;

.../2

- 2 -

(g) to direct the Commissioner to submit to the Minister, once each year and in both official languages, a report on the Commissioner's activities and findings that are not classified, which report the Minister will table in Parliament;

(h) to authorize the Commissioner, at any time the Commissioner considers it advisable, to submit a report containing classified information to the Minister;

(i) to direct the Commissioner, before submitting any report to the Minister, to consult with the Deputy Secretary to the Cabinet (Security and Intelligence) at the Privy Council Office for the purpose of ensuring compliance with all security requirements and the preservation of the secrecy of sources of security and intelligence information and of the security of information provided to Canada in confidence by other nations;

(j) to direct the Commissioner and all persons engaged on his behalf take an oath of secrecy and comply with all applicable government security requirements;

(k) to authorize the Commissioner to engage the services of any staff, advisors and counsel that he considers necessary to assist him in the performance of his duties and functions at such rates of remuneration and reimbursement as may be approved by the Treasury Board;

.../3

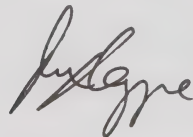
- 3 -

(l) to fix the remuneration of the Commissioner at the per diem rate set out in the annexed schedule, which rate is within the range of \$400 to \$500; and

(m) to authorize that the Commissioner be paid reasonable travel and living expenses incurred by him in the performance of his duties and functions while absent from his ordinary place of residence, in accordance with Treasury Board travel directives;

effective June 19, 1999.

CERTIFIED TO BE A TRUE COPY-COPIE CERTIFIÉE CONFORME



CLERK OF THE PRIVY COUNCIL-LE GREFFIER DU CONSEIL PRIVÉ

Classified Reports, 1996-2001

Classified Report to the Minister - March 3, 1997 (TOP SECRET)

Classified Report to the Minister

- Operational Policies with Lawfulness Implications - February 6, 1998 - (SECRET)

Classified Report to the Minister

- CSE's Activities under *** - March 5, 1998 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- Internal Investigations and Complaints - March 10, 1998 (SECRET)

Classified Report to the Minister

- CSE's activities under *** - December 10, 1998 (TOP SECRET/CEO)

Classified Report to the Minister

- On controlling communications security (COMSEC) material - May 6, 1999 (TOP SECRET)

Classified Report to the Minister

- How We Test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) - June 14, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- A Study of the *** Collection Program - November 19, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- On *** - December 8, 1999 (TOP SECRET - COMINT)

Classified Report to the Minister

- Study of the *** Reporting Process - an overview (Phase I) - December 8, 1999 (SECRET/CEO)

Classified Report to the Minister

- A Study of Selection and *** - an overview - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- CSE's Operational Support Activities Under *** - follow-up - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- Internal Investigations and Complaints - follow-up - May 10, 2000 (SECRET)

Classified Report to the Minister

- On findings of an external review of CSE's ITS Program - June 15, 2000 (SECRET)

Classified Report to the Minister

- CSE's Policy System Review - September 14, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- A study of the *** Reporting Process - Phase II *** - April 6, 2001 (SECRET/CEO)

Classified Report to the Minister

- A study of the *** Reporting Process - Phase III *** - April 6, 2001 (SECRET/CEO)

- Classified Report to the Minister
- A Study of Selection and *** - an overview - 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- CSE's Operational Support Activities Under *** - follow-up - 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- Internal Investigations and Complaints - follow-up - 10 mai 2000 (SECRET)
- Classified Report to the Minister
- On findings of an external review of CSE's ITS Program - 15 juin 2000 (SECRET)
- Classified Report to the Minister
- CSE's Policy System Review - 14 septembre 2000 (TRÈS SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- A study of the *** Reporting Process - Phase II *** - 6 avril 2001 (SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- A study of the *** Reporting Process - Phase III *** - 6 avril 2001 (SECRET/Réservé aux Canadiens)

Rapports classifiés, 1996-2001

Classified Report to the Minister - 3 mars 1997 (TRÈS SECRET)

Classified Report to the Minister
- Operational Policies with Lawfulness Implications - 6 février 1998 - (SECRET)

Classified Report to the Minister
- CSE's Activities under *** - 5 mars 1998 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
- Internal Investigations and Complaints - 10 mars 1998 (SECRET)

Classified Report to the Minister
- CSE's activities under *** - 10 décembre 1998 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- On controlling communications security (COMSEC) material - 6 mai 1999 (TRÈS SECRET)

Classified Report to the Minister
- How We Test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) - 14 juin 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
- A Study of the *** Collection Program - 19 novembre 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
- On *** - 8 décembre 1999 (TRÈS SECRET - COMINT)

Classified Report to the Minister
- A Study of the *** Reporting Process - an overview (Phase I) - 8 décembre 1999 (SECRET/Réservé aux Canadiens)

CLERK OF THE PRIVY COUNCIL--LE GREFFIER DU CONSEIL PRIVE



CERTIFIED TO BE A TRUE COPY--COPIE CERTIFIEE CONFORME

1) à fixer la rémunération du commissaire au
taux journalier établi dans l'annexe
ci-jointe, lequel se situe entre 400 \$ et 500 \$;
m) à autoriser le remboursement des frais de
transport et de séjour raisonnables engagés
par le commissaire lorsque l'exercice de ses
fonctions l'amène à s'éloigner de son lieu de
résidence habituel, conformément aux
directives du Conseil du Trésor concernant
les déplacements;
à compter du 19 juin 1999.

.../3

- que peut approuver le Conseil du Trésor;
- aux taux de rémunération et d'indemnisation,
- besoin pour l'assister dans ses fonctions,
- services de toute personne dont il juge avoir
- k) à autoriser le commissaire à retenir les
- matière de sécurité;
- toutes les exigences du gouvernement en
- un serment de discrétion et se conformant à
- personnes engagées pour son compte prononcent
- J) à exiger que le commissaire et toutes les
- obtenus de pays étrangers;
- sources et la protection des renseignements
- respectées, y compris la confidentialité des
- exigences relatives à la sécurité sont
- Conseil privé pour s'assurer que toutes les
- (Sécurité et renseignements) au Bureau du
- consulter le sous-secrétaire du Cabinet
- présentation de tout rapport au ministre, de
- I) à enjoindre au commissaire, avant la
- renseignements confidentiels;
- par le commissaire, un rapport contenant des
- ministre, et ce à tout moment jugé opportun
- h) à autoriser le commissaire à présenter au
- le ministre au Parlement;
- confidentielle, le rapport devant être déposé par
- constatations qui ne sont pas de nature
- officielles, un rapport sur ses activités et ses
- ministre, une fois l'an et dans les deux langues
- g) à enjoindre au commissaire de présenter au



PRIVY COUNCIL • CONSEIL PRIVÉ

Sur recommandation du ministre de la Défense nationale et en vertu de la partie II de la Loi sur les enquêtes, Son Excellence le Gouverneur général en conseil autorise le ministre de la Défense nationale (le « ministre ») :

a) à reconduire l'honorable Claude Bisson, de Montréal (Québec), dans ses fonctions de commissaire du Centre de la sécurité des télécommunications (le « CST ») pour une période de trois ans pendant laquelle il examinera les activités du CST et s'assurera qu'elles sont conformes à la loi;

b) à autoriser le commissaire à entreprendre cet examen de sa propre initiative ou à la requête du ministre;

c) à autoriser le commissaire à instruire toute plainte concernant la légalité des activités du CST que pourrait déposer un citoyen canadien ou un résident permanent du Canada;

d) à autoriser le commissaire à ne pas instruire une plainte lorsque, de l'avis de celui-ci, il existe d'autres recours légaux;

e) à autoriser expressément le commissaire à informer toute personne ayant déposé une plainte des résultats de l'enquête qui a été effectuée, en prenant soin de ne divulguer aucun renseignement confidentiel à cette personne;

f) à enjoindre au commissaire de signaler au ministre et au procureur général du Canada toute activité du CST qu'il estime ne pas être conforme à la loi;

Le budget qui m'avait été alloué pour l'année financière 2000-2001 était de 648 800 \$. Je suis en mesure de signaler qu'il a bien suffi à couvrir les dépenses réelles engagées.

Mon bureau se compose toujours de deux employés à plein temps et de plusieurs spécialistes dont je retiens les services par contrat. À l'heure actuelle, cinq personnes effectuent des travaux spécialisés selon cette formule, et toutes possèdent l'autorisation sécuritaire requise. Cette façon de procéder m'assure la continuité et la souplesse voulues pour obtenir les compétences dont j'ai besoin afin d'examiner efficacement les activités du CST.

COUP D'ŒIL SUR L'AVENIR

Sauvegarder la vie privée des Canadiens

Comme je l'ai déjà fait remarquer, la technologie de collecte de renseignements sur l'étranger du CST doit se perfectionner constamment pour suivre le rythme du progrès des technologies de communication. Malgré la plus grande efficacité des nouvelles technologies, il reste probable que le CST recevra involontairement de petites quantités de communications canadiennes. De plus, chaque nouveau système ou technique de collecte mis en service semble comporter cette possibilité. Cependant, le CST est bien conscient du fait qu'il doit constamment étendre ses moyens d'écarter les communications canadiennes, ou risquer d'agir illégalement s'il ne fait pas tous ses efforts dans ce sens.

À cet égard, j'ai informé le CST que, en plus de mes autres activités d'examen, je chercherai à m'assurer qu'il utilise toutes les technologies nouvelles pour veiller à sauvegarder la vie privée des Canadiens.

d'ordres du ministre. J'applaudis cette initiative, car elle renforcera les liens de responsabilité entre le CST et le ministre de la Défense nationale, qui est comptable de l'organisme devant le Parlement.

Mon mandat m'autorise à enquêter sur les plaintes déposées par des Canadiens ou des résidents permanents du Canada au sujet des activités du CST. Des demandes de renseignements officielles ont été faites en 2000-2001, mais aucune n'a abouti à une plainte officielle.

Au cours de l'année dernière, mon bureau a entretenu des contacts officiels au sein de la communauté de la sécurité et du renseignement. Nous avons été particulièrement heureux d'accueillir l'inspecteur général de l'Afrique du Sud pendant sa tournée de l'automne 2000 en Amérique du Nord. J'envisage par ailleurs avec plaisir de renouveler connaissance avec mes homologues d'autres pays lors de la prochaine conférence des organismes d'examen, à Washington, en octobre 2001.

Je suis convaincu que, au cours de la période à l'examen, le CST a agi conformément à la loi dans l'exécution de son mandat, et qu'il n'a pas ciblé les communications de citoyens ni de résidents permanents du Canada. Je fais cette affirmation en me fondant sur l'examen approfondi de ses activités effectué pendant l'année.

Mon mandat m'oblige à informer le ministre de la Défense nationale et le procureur général du Canada de toute activité du CST qui, à mon sens, n'est peut-être pas conforme à la loi. Je n'ai pas eu à faire cela jusqu'ici. Le CST est conscient des limites qui lui sont imposées, il reçoit les avis de conseillers juridiques affectés auprès de l'organisme par le ministère de la Justice, et il dispose de politiques et de procédures destinées à promouvoir la légalité. Ces mesures se sont révélées efficaces.

Autres activités

Constations faites en 2000-2001

Pouvoirs en matière de politiques

J'ai constaté que ces autorisations ne constituent pas une obligation de détruire des documents et qu'elles ne donnent aucune indication quant au moment où ceux-ci doivent être détruits. Par ailleurs, elles ne prévoient ni n'autorisent de périodes de conservation des documents. Les périodes de conservation et d'élimination sont déterminées par le ministre responsable de l'institution et doivent, bien entendu, être conformes à toute autre loi applicable.

J'ai acquis la conviction que les politiques du CST se conformant aux exigences des lois et des politiques relatives à la gestion des fonds de renseignements du gouvernement. Je recommande toutefois que le CST s'occupe en priorité de compléter ses calendriers de conservation et d'élimination.

Dans mon rapport annuel de 1998-1999, je signalais mon intention d'examiner le nouveau cadre de pouvoirs, de responsabilités et de coordination touchant les politiques, que le CST avait adopté peu auparavant. Je m'intéressais plus particulièrement à deux des objectifs de ce cadre, soit déterminer le palier approprié pour différentes politiques, et procurer un niveau souhaitable de souplesse opérationnelle pour les activités quotidiennes.

Au cours de l'année passée, j'ai examiné le nouveau cadre, et je l'ai trouvé bien conçu et judicieux. Il faudra cependant du temps pour y adapter toutes les politiques de l'organisme. S'il subsiste certaines lacunes, le CST dispose de politiques pour ses besoins essentiels, et le nouveau système devrait répondre à mon souci antérieur de trouver les politiques au bon palier de l'organisation et de les voir approuvées au niveau approprié.

Au cours de l'année à l'étude, j'ai appris avec plaisir que des fonctionnaires avaient entamé des entretiens dans le but de faire communiquer les politiques internes de base au CST sous la forme

Au cours de l'année écoulée, j'ai continué à examiner les activités du CST sous l'angle de leurs rapports avec le cycle du renseignement, ainsi qu'avec le traitement et la production des produits du renseignement. Comme je le mentionnais dans mon dernier rapport annuel, le CST examine quotidiennement les transmissions brutes qu'il reçoit de nombreuses sources et en évalue la valeur sur le plan du renseignement étranger par rapport aux priorités du gouvernement. Il communique ensuite les résultats de ce travail à ses clients du gouvernement sous la forme de produits du renseignement.

L'année passée, j'ai examiné les politiques et les pratiques de traitement liées à la réception et à la conservation des transmissions de renseignements sur l'étranger. Je me suis penché sur la façon dont le CST reconnaît les questions présentant un intérêt en matière de renseignements dans les transmissions brutes qu'il reçoit, et sur les pratiques liées à leur conservation et à leur diffusion subséquente sous la forme de rapports de renseignement. Et, comme je le fais d'habitude, j'ai examiné les politiques et les pratiques du CST qui, dans ce cycle d'activités, visent expressément à sauvegarder la vie privée des Canadiens.

J'ai en outre examiné les politiques de gestion de l'information du CST à la lumière de la *Loi sur les archives nationales* du Canada ainsi que de la politique et des lignes directrices du Conseil du Trésor touchant la gestion des fonds de renseignements.

Les ministères et organismes sont tenus d'établir des autorisations de disposition de documents pour leurs fonds de renseignements opérationnels et administratifs. Ces autorisations leur permettent de se débarrasser de certains fonds de renseignements et les obligent à transmettre aux Archives nationales d'autres fonds présentant un intérêt archivistique, pour y être conservés.

légalité. Il effectue ensuite, avec mon autorisation, des examens systématiques de ces activités. Je communique les résultats de ces examens au ministre de la Défense nationale sous la forme de rapports classifiés. La production d'un rapport classifié n'indique pas que j'ai découvert un cas d'illégalité. Elle indique plutôt que le rapport renferme des renseignements de nature délicate qui nécessitent cette classification.

Les travaux de recherche et de préparation qu'exigent mes rapports au ministre représentent le gros du travail de mon bureau et me procurent une information détaillée touchant divers aspects des activités du CST.

J'ai examiné les autorisations en vertu desquelles le CST recueille des renseignements sur l'étranger au nom du gouvernement du Canada, ainsi que son mandat de protéger la sécurité des technologies de l'information du gouvernement. Et j'examine régulièrement ses politiques, directives et pratiques afin de m'assurer qu'elles contribuent à la légalité de ses activités et à la protection de la vie privée des Canadiens.

Mes examens ont porté, entre autres, sur la façon dont le CST fournit des rapports de renseignements à ses clients, et sur la réception de renseignements de ses partenaires des Secondes Parties. Je surveille régulièrement les activités opérationnelles de l'organisme, ainsi que les circonstances ayant mené à des enquêtes sur la sécurité interne.

On trouvera à l'annexe B la liste des rapports classifiés que j'ai communiqués au ministre depuis ma nomination, en 1996.

Le rôle du commissaire

EXAMEN DU CST

Le CST s'est fixé trois buts stratégiques pour les 10 prochaines années :

- être reconnu comme le centre d'excellence du gouvernement pour ce qui est de l'analyse et de l'exploitation des capacités du réseau mondial;
- protéger l'infrastructure d'information du Canada et veiller à son bon fonctionnement;
- moderniser les produits et les services du CST ainsi que leur mode de prestation.

Dans un premier temps, le CST a renforcé les liens entre ses programmes de SIGINT et de STI. Même si leurs activités ont un rapport entre elles, ces deux programmes ont toujours fonctionné indépendamment l'un de l'autre. Pour atteindre ses buts stratégiques, le CST a l'intention d'exploiter les synergies créées par le rapprochement des deux programmes. En examinant les vulnérabilités des systèmes de communication et d'information ensemble, les experts du SIGINT et de la STI mettent maintenant leur savoir en commun pour repérer les menaces visant les systèmes canadiens, ainsi que les occasions de recueillir des renseignements sur l'étranger.

En juin 2000, le chef du CST m'a présenté un exposé sur ce sujet. Par la suite, mon bureau a examiné la stratégie dans le détail avec la haute direction de l'organisme. Je ne pense pas que cela modifiera fondamentalement la façon dont j'examine les activités du CST, car je continuerai d'en juger la légalité. Entre-temps, j'ai exprimé mon appui pour cette entreprise.

Mon mandat d'examiner les activités du CST et de faire rapport au ministre de la Défense nationale est exposé dans un décret (voir annexe A).

Chaque année, mon bureau recense des secteurs des activités du CST où, de prime abord, on pourrait présumer qu'il se pose des questions de

Le plan stratégique du CST

- Le nombre d'attaques dirigées contre les réseaux et les systèmes gouvernementaux est en hausse. Selon une estimation contenue dans une étude effectuée en septembre 2000 sur les menaces visant les sites Internet fédéraux, un site typique fait l'objet de 10 incidents de menace ou plus chaque semaine. De plus, la fréquence des attaques contre les systèmes américains provenant du Canada ou passant par notre pays commence à poser problème.
- Le nouveau Bureau de la protection de l'infrastructure essentielle et de la planification d'urgence, dont la création a été annoncée par le gouvernement en février 2001 et qui est chargé d'élaborer et de mettre en œuvre un plan complet de protection de l'infrastructure essentielle du Canada, comptera sur le soutien technique du CST.

Pendant l'année examinée, le CST a entrepris un important travail stratégique afin de trouver de nouvelles manières d'exécuter son mandat.

À cette fin, il a d'abord défini sa vision, soit : « être l'organisme qui maîtrise le réseau mondial d'information afin d'accroître la sécurité et la prospérité du Canada ». Ce faisant, le CST est effectivement retourné à ses origines en reconnaissant que sa force de base réside dans sa capacité de comprendre et de protéger les communications et les systèmes de communication. Sa capacité d'exploiter ces systèmes pour fournir des renseignements sur l'étranger découle de cette force de base.

Pour soutenir sa vision, le CST vise à devenir un centre d'excellence qui développera et appliquera ses compétences techniques et sa connaissance des réseaux de communication mondiale, et il compte aider le Canada à répondre à ses besoins d'information essentiels.

Le CST doit composer avec le rythme révolutionnaire de l'évolution technologique. Le fondement de ses activités est la technologie, qui touche l'organisme, et ses partenaires, de plusieurs façons :

- Les canaux de transmission des communications étrangères se multiplient. Les nouvelles techniques de communication sans fil, par fibres optiques et par Internet continuent de progresser, ce qui oblige les informaticiens et les ingénieurs du CST à accroître et étendre constamment leurs connaissances.

- Les cibles des activités de collecte de renseignements sur l'étranger, dont les groupes terroristes, ont maintenant facilement accès aux produits sophistiqués d'une industrie des télécommunications représentant plusieurs billions de dollars, y compris la technologie de chiffrement numérique, qui est disponible à titre de logiciel public sur Internet, de sorte qu'il est difficile, sinon impossible, de déchiffrer leurs communications.

- De plus en plus, des quantités énormes d'information sont achevinées sur les nouveaux canaux de communication, de sorte que le CST doit affecter un personnel très nombreux pour déceler les renseignements utiles.

- Les ministères et organismes du gouvernement canadien emploient aussi de nouveaux modes de communication interconnectés avec des systèmes informatiques contenant des renseignements de nature délicate, ou qui contrôlent des infrastructures essentielles. Ils comptent sur les experts du CST en matière de STI pour leur donner des conseils afin de protéger leurs réseaux de communication et leurs systèmes informatiques.

Les forces canadiennes qui s'engagent dans des opérations de maintien de la paix à l'étranger comprennent mieux la situation sur le terrain grâce aux renseignements fournis par le CST.

Le CST fournit à ses clients du gouvernement chargés de protéger la sûreté publique de l'information tirée des renseignements sur l'étranger, qui contribuent aux efforts de lutte contre le terrorisme, la prolifération des armes, le trafic de la drogue, la migration illégale et la criminalité transnationale. Plus récemment, il a commencé à fournir aux mêmes organismes une assistance technique.

Le CST collabore étroitement avec le Groupe des opérations d'information des Forces canadiennes (GOIFC), afin d'améliorer l'appui qu'offre directement le Groupe dans le cadre des opérations militaires du Canada. (Créé en avril 1998, le GOIFC regroupe divers éléments du ministère de la Défense nationale, notamment le Réseau radio supplémentaire des Forces canadiennes. Il constitue un centre névralgique pour les opérations d'information.)

Dans le cadre de son programme de STI, le CST continue d'encourager et d'aider des entreprises canadiennes à mettre au point de nouveaux produits de sécurité. Il entretient par ailleurs des relations suivies avec plusieurs ministères et organismes et les aide à évaluer leurs besoins en matière de STI à mesure qu'ils s'orientent vers la prestation de services en ligne.

Le CST a fourni une expertise de niveau supérieur au Groupe de travail du gouvernement sur la protection des infrastructures essentielles. Ce groupe de travail, créé en avril 2000, a recommandé les mesures que le gouvernement fédéral devrait prendre pour protéger la partie de l'infrastructure du Canada qui est essentielle à la santé, à la sûreté, à la sécurité et au bien-être économique des Canadiens.

Contributions récentes du CST

Contrôle des activités du CST

Nouvelle-Zélande. Ces arrangements, qui ont été officialisés après la Deuxième Guerre mondiale et maintenus durant la guerre froide, permettent l'échange de renseignements électromagnétiques, de technologies et d'information au sujet de sources et de techniques d'intérêt commun.

Dans le cadre de mon travail régulier d'examen des activités du CST, je peux affirmer que celui-ci ne sert pas de ses partenaires pour contourner les lois du Canada, et qu'il ne leur fournit pas de communications qu'ils ne pourraient pas recueillir légalement eux-mêmes.

En me fondant sur les travaux d'examen que j'ai effectués jusqu'ici, je constate que les activités du CST sont guidées par la loi, par ses principes généraux et par les priorités du gouvernement, et non par les moyens techniques dont il dispose. En plus de mes propres examens, le CST est par ailleurs assujéti à l'examen indépendant de nombreuses instances, notamment les tribunaux, le commissaire à la protection de la vie privée, le commissaire à l'information, la Commission canadienne des droits de la personne et le vérificateur général du Canada.

Les réseaux actuels de communication mondiale génèrent une quantité excessive d'information à laquelle le CST doit faire face. Cette quantité est en soi un contrôle. D'un point de vue pratique, le CST doit rester concentré sur son mandat s'il veut répondre aux priorités qui lui sont assignées en matière de renseignement sur l'étranger.

Le gouvernement utilise les rapports de renseignement du CST pour favoriser les intérêts économiques et politiques du Canada dans ses relations avec les États étrangers.

La sécurité des technologies de l'information

Ces dernières années, le développement et la mise en œuvre de nouvelles technologies ont transformé l'orientation et la complexité des activités entreprises par le CST, dans le cadre de son programme de STI, afin de protéger les communications et les systèmes de communication du gouvernement.

renseignement sur l'étranger à ses clients du gouvernement du Canada. Plus de 100 000 rapports de SIGINT sont mis à la disposition de ceux-ci chaque année.

Jusqu'à récemment, le matériel informatique, les logiciels et les réseaux n'étaient pas encore très répandus et n'avaient qu'une application limitée. À l'heure actuelle, cependant, l'ordinateur s'est imposé comme moyen de communication entre les gens et il est à l'origine de nombreuses technologies qui forment l'infrastructure canadienne en matière d'information critique.

Ce contexte a fait apparaître, dans les systèmes d'information du gouvernement, de nouvelles vulnérabilités qui exigent des solutions nouvelles permettant de parer aux menaces à la sécurité et à la vie privée.

Le gouvernement compte sur le CST pour protéger l'information stockée dans ses systèmes informatiques ou transmise par ceux-ci, tandis que divers ministères et organismes s'appliquent à mettre une multiplicité de services en ligne à la disposition du public. Parallèlement, la loi exige que les renseignements personnels au sujet des Canadiens soient protégés, alors que les systèmes informatiques du gouvernement sont de plus en plus interreliés et vulnérables aux perturbations et à des menaces comme les dénis de service.

Relations avec les alliés

Le Canada profite d'arrangements de longue date conclus entre le CST et ses homologues des États-Unis, du Royaume-Uni, de l'Australie et de la

Le programme de SIGINT du CST est guidé par les priorités en matière de renseignement sur l'étranger établies annuellement par la réunion des ministres sur la sécurité et le renseignement, que préside le Premier ministre.

Pour s'acquitter de son mandat en matière de SIGINT, le CST recueille les signaux émis par divers modes de communication de pays étrangers. La collecte et le traitement de ces signaux font intervenir des technologies très sophistiquées et très complexes. Le traitement comprend souvent le déchiffrement et la traduction de communications chiffrées pour les rendre intelligibles. Le chiffrement relève de la cryptologie, science qui utilise des algorithmes mathématiques pour dissimuler ou déguiser des communications.

Le CST m'a informé que les progrès accomplis dans le domaine des transmissions mondiales présentent des défis permanents à la collecte et au traitement des signaux étrangers. Les quantités énormes de signaux de communications produits quotidiennement, alliées au recours accru aux logiciels de chiffrement et à la disponibilité publique de ceux-ci, ne font qu'ajouter à ces défis.

En conséquence, le CST a consacré des ressources additionnelles à la recherche et au développement de techniques de collecte et de traitement des communications, afin que le gouvernement puisse être tenu au courant des menaces visant les intérêts du Canada. À cette fin, le CST fait appel à un ensemble de spécialistes, dont des informaticiens, des mathématiciens et des linguistes. Il a en outre besoin d'analystes du renseignement bien au fait de questions comme les affaires politiques, économiques et militaires internationales, le terrorisme et la criminalité transnationale, afin de produire des rapports de renseignement. Ces rapports sont le moyen par lequel le CST communique l'information relative au

consultation avec les parties intéressées par son activité, une nouvelle approche stratégique relativement à son mandat.

Tel est le contexte dans lequel je continue d'examiner les activités du CST, afin de déterminer leur conformité aux lois du Canada, et d'évaluer les efforts qu'il déploie pour sauvegarder la vie privée des Canadiens.

Comme je l'ai fait les années précédentes, j'examine dans le présent rapport la façon dont le CST s'est acquitté de son mandat au cours de l'année écoulée.

Le CST est un organisme du ministère de la Défense nationale, qui aide le gouvernement dans deux domaines distincts, mais liés entre eux :

- Il fournit au gouvernement des renseignements sur l'étranger en recueillant et analysant les signaux radio, radar et autres signaux électroniques de pays étrangers et en lui communiquant des rapports à ce sujet (renseignement électromagnétique ou SIGINT).
- Il contribue à faire en sorte que les télécommunications et les technologies de l'information du gouvernement canadien soient protégées contre l'interception, la perturbation, la manipulation et le sabotage (sécurité des technologies de l'information ou STI).

Le ministre de la Défense nationale est pleinement comptable du CST devant le Parlement. Il est soutenu à cet égard par deux hauts fonctionnaires, soit le sous-ministre de la Défense nationale, pour les questions financières et administratives, et le sous-greffier du Conseil privé, conseiller juridique et coordonnateur de la sécurité et du renseignement, pour les affaires stratégiques et opérationnelles.

Mandat

LE CST AUJOURD'HUI

Au cours des cinq années écoulées depuis ma première nomination, j'ai vu naître des technologies de communication mondiale complexes, parallèlement à l'évolution des réalités politiques, sociales et économiques. Cette situation a mis en évidence de nouvelles menaces à la sécurité, à la défense et aux intérêts nationaux du Canada et fait ressortir le besoin pressant pour le gouvernement du Canada de déterminer comment parer à ces menaces.

Au cours de la même période, le Centre de la sécurité des télécommunications (CST) s'est efforcé d'entretenir sa capacité de répondre aux priorités du gouvernement en matière de renseignement sur l'étranger à mesure de leur évolution, et de protéger l'intégrité de ses systèmes de communication et d'information.

Je suis convaincu que, si les capacités du CST n'étaient pas entretenues comme il convient, les intérêts nationaux du Canada seraient gravement compromis. Par exemple, si le CST n'était pas en mesure de faire rapport sur les activités et les intentions d'États et d'individus étrangers, le bien-être politique et économique du Canada serait menacé. De plus, si le CST ne pouvait plus protéger les systèmes d'information et les fonds de renseignements du gouvernement, les efforts de celui-ci seraient paralysés dans les domaines de la prestation électronique des services et du commerce électronique, ce qui nuirait finalement à la compétitivité économique du Canada.

Les progrès technologiques se poursuivront certainement et pourraient même s'accélérer. La haute direction du CST m'a informé de sa conviction que celui-ci doit réorienter ses efforts pour s'acquitter de ses responsabilités envers le gouvernement, faute de quoi il risque d'être à la traîne. En conséquence, le CST a adopté, en

TABLE DES MATIÈRES

1	Introduction
2	Le CST aujourd'hui.....
2	• Mandat
3	• Le renseignement électromagnétique
4	• La sécurité des technologies de l'information
4	• Relations avec les alliés
5	• Contrôle des activités du CST
5	• Contributions récentes du CST
7	Evolution du CST
7	• Des pressions dans le sens du changement.....
8	• Le plan stratégique du CST
9	Examen du CST
9	• Le rôle du commissaire.....
11	• Activités de l'année 2000-2001
11	• Produits du renseignement sur l'étranger.....
11	• Gestion de l'information
12	• Pouvoirs en matière de politiques
13	• Autres activités
13	• Constatations faites en 2000-2001.....
14	• Personnel et budget
14	Coup d'œil sur l'avenir.....
14	• Sauvegarder la vie privée des Canadiens
15	Annexe A : Mandat du commissaire
19	Annexe B : Rapports classifiés, 1996-2001

Communications Security
Establishment Commissioner



CANADA

The Honourable Claude Bisson, O.C.



Mai 2001

L'honorable Arthur C. Eggleton, C.P.
Ministre de la Défense nationale
Édifice Mgén G.R. Pearkes, 13^e étage
101, promenade Colonel By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément à l'alinéa g) du décret C.P. 1999-1048 prévoyant le renouvellement de ma nomination au poste de commissaire du Centre de la sécurité des télécommunications, j'ai le plaisir de vous soumettre mon rapport annuel pour l'année 2000-2001, qui fait état de mes activités et constatations, pour présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.



Claude Bisson

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R6
(613) 992-3044 Fax: (613) 992-4096

Bureau du Commissaire du Centre de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044
Téléc. : (613) 992-4096

© Ministère des Travaux publics et des Services gouvernementaux Canada 2001
ISBN 0-662-65817-5
N° de cat. D95-2001

Commissaire
du Centre
de la sécurité
des télécommunications

Rapport
annuel



2000
↑
2001



Canada

CA1
ND800
-S16

Communications
Security
Establishment
Commissioner

Annual Report

2001
↓
2002



Canada

Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station 'B'
Ottawa, Ontario
K1P 5R5

Tel: (613) 992-3044
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 2002
ISBN 0-662-66619-4
Cat. No. D95-2002

Communications Security
Establishment Commissioner



Commissaire du Centre de la
sécurité des télécommunications

The Honourable Claude Bisson, O.C.

L'honorable Claude Bisson, O.C.

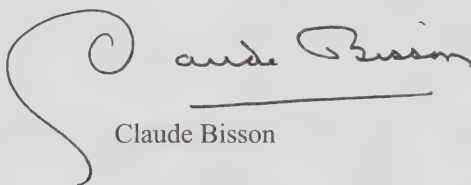
June 2002

The Honourable John McCallum, P.C.
Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Mr. McCallum:

Pursuant to sub-section 273.63 (3) of the *National Defence Act*, I am pleased to submit to you my 2001-2002 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,



Claude Bisson



TABLE OF CONTENTS

Introduction	1
The Anti-terrorism Act	2
• More than a decade of debate	3
• Communications Security Establishment mandate	4
• Ministerial authorization.....	5
• The Commissioner's mandate.....	7
• Public interest defence	7
• Implications for the Commissioner	8
2001-2002 Activities	9
• Anti-terrorism legislation.....	9
• Classified reports	10
• Complaints	10
• 2001-2002 findings	10
The Year Ahead	10
• The Public Safety Act	10
• Budget and staff	11
• Commissioner's reappointment	11
• Review agencies conference	12
Looking Ahead	12
• Safeguarding the privacy of Canadians	12
Annex A: Commissioner's Mandate	13
Annex B: Classified Reports, 1996-2002	17

INTRODUCTION

Since my last annual report was released in May 2001, the context in which Canada's security and intelligence community works has been transformed. Members of the Canadian Forces have gone into action in Afghanistan. Our closest neighbour is still recovering from the terrorist attacks of September 11. Police and intelligence officials are working across Canada and with their counterparts elsewhere to prevent further terrorist activity in this country and abroad.

This new environment has given Canadians a growing awareness of the contributions to our well-being that are made by the members of our security and intelligence community, as well as police, fire services, enforcement officials, and military forces. Canadians rely on them to detect threats to public safety and to stop those who want to harm us or our allies.

The agency I review – the Communications Security Establishment (CSE) – joined other security and intelligence organizations in responding to the events of the past nine months. CSE provides the government with foreign intelligence by collecting, analyzing and reporting on information such as electronic emissions and data it acquires from the global information infrastructure (signals intelligence). It also helps ensure that the Canadian government's electronic information and its infrastructure are secure from interception, disruption, manipulation or sabotage (information technology security).

In the immediate aftermath of September 11, CSE employees worked around the clock to contribute to the worldwide effort to identify those responsible for the attacks in the United States and to prevent additional attacks. Together with other members of Canada's security and intelligence community, CSE formed new partnerships in common cause against the threat of terrorism.

The Government of Canada quickly reaffirmed terrorism as a matter of national concern affecting the security of the nation. Noting that “the challenge of eradicating terrorism, with its sophisticated and trans-border nature, requires enhanced international cooperation and a strengthening of Canada’s capacity to suppress, investigate and incapacitate terrorist activity,”¹ the government introduced into Parliament last October its omnibus Bill C-36, the *Anti-terrorism Act*.²

To strengthen Canada’s ability to combat terrorism, and to respond to threats to Canadian lives and interests from terrorism, the Bill proposed several amendments to existing Acts. Of particular interest to me were the proposed amendments to the *Official Secrets Act* and the *National Defence Act*, the latter providing the legislative basis for both the activities of CSE and the role of the CSE Commissioner. Bill C-36, which was passed by Parliament and proclaimed on December 24, 2001, also introduced new elements to the roles of CSE and my Office.

In this year’s annual report, I describe those parts of the legislation that affect CSE and the Commissioner and the implications of the legislation. As required by my mandate I also report on the 2001-2002 activities and findings of my Office.

THE ANTI-TERRORISM ACT

The *Anti-terrorism Act* is a major piece of legislation with numerous elements affecting many areas of government activity. Despite concerns expressed about the haste with which the legislation was drafted and debated, I know with certainty that those parts of the legislation that deal with CSE and

¹ From the preamble to Bill C-36, the *Anti-terrorism Act*, S.C. 2001, c. 41.

² The *Anti-terrorism Act*: An Act to amend the Criminal Code, the *Official Secrets Act*, the *Canada Evidence Act*, the *Proceeds of Crime (Money Laundering) Act* and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism.

the CSE Commissioner benefited from years of discussion within government long before September 11.

More than a decade of debate

As long ago as 1990, the House of Commons Special Committee on the Review of the *Canadian Security Intelligence Service Act* and the *Security Offences Act* recommended that Parliament establish CSE by statute. Although the government chose not to act on the recommendation at that time, it did indicate that it was “considering providing the Minister of National Defence with some additional capacity for review of CSE.” This ultimately led to my appointment in 1996 as the first Commissioner of CSE.

The issue of legislation for CSE arose again in 1996 when the Privacy Commissioner completed his examination of CSE. He concluded that, to the extent it could be established through his audit, CSE operated in compliance with the *Privacy Act* and the principles of fair information practices. However, he too recommended the enactment of enabling legislation for CSE.

Later that year, the Auditor General of Canada tabled a report on the Canadian intelligence community in which he called on the government to consider the advantages of an appropriate legislative framework for CSE. He reiterated this view in a short 1998 follow-up report.

Similarly, in 1999, the Senate Committee on Security and Intelligence, chaired by former Senator William Kelly, recommended that CSE have its own Act of Parliament and that the legislation provide for a permanent and separate review body for CSE.

In four of my annual reports, I raised the matter of legislation for CSE. I expressed the view, in these

reports and elsewhere, that legislation would be an appropriate development that would put CSE on a firm footing by articulating its mandate and powers and its relationships with Parliament, the government, and the Minister of National Defence.

Suddenly and unexpectedly, what had been discussed for many years became a reality. The government accepted the advice of its independent observers and agreed that, in the context of the omnibus Bill C-36, the time was right to introduce legislation for CSE and the CSE Commissioner.

In my view, the passage of legislation dealing with CSE and the Commissioner is a welcome development. Moreover, I believe the legislation appropriately takes into account the critical balance between the needs of the state to collect information to protect its citizens and the individual rights of those citizens to privacy.

The parts of the Act that relate to CSE and the Commissioner are described below.

Communications Security Establishment mandate

The *Anti-terrorism Act* provides a legislative base for CSE by amending the *National Defence Act*. The new section 273.64 of the *National Defence Act* states:

- (1) The mandate of the Communications Security Establishment is
 - (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
 - (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and

(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

(2) Activities carried out under paragraphs (1)(a) and (b)

(a) shall not be directed at Canadians or any person in Canada; and

(b) shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

These provisions have the effect of enshrining in legislation the historical activities of CSE.

Ministerial authorization

The *National Defence Act* also allows the Minister of National Defence to authorize CSE to intercept private communications in specific circumstances, by issuing a written Ministerial authorization. The Minister may, for the sole purpose of obtaining foreign intelligence, issue an authorization if satisfied that:

- (a) the interception will be directed at foreign entities located outside Canada;
- (b) the information to be obtained could not reasonably be obtained by other means;
- (c) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and
- (d) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

In the past, CSE was prohibited from intercepting any communication in which one of the participants in the communication was in Canada – even if the target of the interception was outside Canada. This new provision allows the Minister of National Defence to authorize such interceptions in circumstances defined in the authorization. An example might be a communication in which a person of foreign intelligence interest in another country contacts a counterpart in Canada.

The new legislation also allows the Minister to issue authorizations to intercept private communications “for the sole purpose of protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference.” Section 273.65 (4) of the *National Defence Act* sets out the conditions for such an authorization:

- (a) the interception is necessary to identify, isolate or prevent harm to Government of Canada computer systems or networks;
- (b) the information to be obtained could not reasonably be obtained by other means;
- (c) the consent of persons whose private communications may be intercepted cannot reasonably be obtained;
- (d) satisfactory measures are in place to ensure that only information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks will be used or retained; and
- (e) satisfactory measures are in place to protect the privacy of Canadians in the use or retention of that information.

The legislation directs the CSE Commissioner to review the activities carried out under Ministerial authorizations to ensure they are authorized and to report annually to the Minister on the review.

The Commissioner's mandate

In addition to assigning responsibility for reviewing CSE's activities under Ministerial authorizations, the *National Defence Act* now sets out the duties of the Commissioner's office as follows:

- (a) to review the activities of the [CSE] to ensure that they are in compliance with the law;
- (b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and
- (c) to inform the Minister [of National Defence] and the Attorney General of Canada of any activity of the [CSE] that the Commissioner believes may not be in compliance with the law.

In effect, the mandate I have been fulfilling since 1996 by Order in Council is now entrenched in law.

Public interest defence

The *Anti-terrorism Act* also made significant changes in the former *Official Secrets Act*, now called the *Security of Information Act*. The Act now prohibits people bound by secrecy from communicating or confirming "special operational information", which is defined to include information about the kinds of activities CSE lawfully undertakes.

A person would not be found guilty of an offence under this part of the Act, however, if that person could establish that he or she acted in the public interest by communicating or confirming special operational information. The Act states that a person acts in the public interest if the person's purpose is to disclose "an offence under an Act of Parliament that he or she reasonably believes has been, is being or is about to be committed by another person in the purported performance of that person's duties and functions for, or on behalf of, the Government of Canada." The public interest in

disclosure must outweigh the public interest in non-disclosure. This is why it is called a public interest defence.

A judge or court can consider a public interest defence only if the person involved, before disclosing special operational information, brought his or her concerns to the attention of the institution's deputy head or the Deputy Attorney General of Canada. If a person with a concern about CSE's activities does not receive a response from the deputy head or Deputy Attorney General within a reasonable time, he or she must then bring the concern to the CSE Commissioner and must allow a reasonable time for the Commissioner to respond. Failure to do so precludes that person from using the public interest defence.

Implications for the Commissioner

It will take some time to fully assess the implications of the *Anti-terrorism Act* for my work. The responsibility of reviewing CSE activities under Ministerial authorizations is a significant one. These authorizations will extend CSE's activities into new areas, and I will want to ensure that CSE has appropriate policies and procedures in place, and that it applies them, to protect the privacy of Canadians as it implements this expanded mandate.

The Commissioner's role in public interest defence cases is comparable in some ways to my continuing responsibility to consider complaints about CSE, and I anticipate that the measures I have in place to address complaints will allow me to respond quickly and appropriately to any concerns raised about CSE's activities under the *Security of Information Act*. Very few complaints about CSE have been brought to me since I took office in 1996. It remains to be seen whether the new public interest defence provisions will generate additional activity.

With the Commissioner's mandate now clearly established in law, I will no longer need to debate the theoretical merits of one arrangement for reviewing CSE over another. However, the Commissioner's new status as an ongoing institution of government raises a host of practical administrative issues that must now be addressed. For one thing, I will need to ensure my Office is sufficiently resourced to review CSE's expanded activities. Other issues, such as the Office's place in government, must also be explored in coming months.

2001-2002 ACTIVITIES Anti-terrorism legislation

As Parliamentarians considered the *Anti-terrorism Act* last autumn, they sought my views on the parts of the legislation dealing with CSE and the CSE Commissioner. I appeared in October 2001 before the Special Senate Committee on the Subject Matter of Bill C-36, and in November I submitted a brief to the House of Commons Standing Committee on Justice and Human Rights. The texts of my opening remarks to the Senate Committee and my brief to the House of Commons Committee are available on my Office's website at <http://csec-ccst.gc.ca>.

Since the passage of the legislation, my staff and I have focused on my new responsibilities. Most significantly, I began preparations early in 2002 to launch my first review of CSE's activities under Ministerial authorization issued by the Minister of National Defence. I will be reporting the results to the Minister later this year.

Between the passage of the legislation and the end of the 2001-2002 fiscal year, I received no requests to consider concerns about the activities of CSE from persons seeking to establish a public interest defence under the *Security of Information Act* as it relates to the disclosure of special operational information.

Classified reports

My mandate authorizes me to submit classified reports to the Minister about CSE's activities. Since my appointment in 1996, I have submitted 19 such reports, including two in 2001-2002, and two others were nearing completion at year's end. The inquiries I made to produce these reports revealed no evidence of unlawful activity by CSE. A complete list of the classified reports I have submitted to the Minister can be found in Annex B.

Complaints

During 2001-2002, I received one complaint from a member of the public concerning CSE. I reviewed this complaint and determined that no further action was required.

2001-2002 findings

Each year in this report I state my findings about the lawfulness of CSE's activities based upon the results of a series of reviews. These reviews include, but are not limited to, an examination of the legal authorities under which CSE conducts its activities as well as related policies and practices.

I am able to report that I am satisfied that those CSE activities examined during the period under review complied with law and existing policy. Further, I found no evidence that CSE targeted the communications of Canadian citizens or permanent residents.

THE YEAR AHEAD

The Public Safety Act

In April 2002 the government introduced Bill C-55, the *Public Safety Act*. Still under consideration by Parliament as I write this, the Bill is a companion piece to the *Anti-terrorism Act* passed in December 2001. Bill C-55 proposes legislative changes on a wide range of subjects, from transportation safety and immigration to biological weapons.

Of particular interest to me is a proposed amendment to the *National Defence Act* that would confer a new responsibility on the Commissioner of CSE for reviewing activities undertaken by the Department of National Defence or the Canadian Forces to protect their computer networks and systems.

Over the coming months, I will review this new legislative provision and the impact it may have on my office.

Budget and staff

During the 2001-2002 fiscal year, my budget allocation was \$647,150. I can report that actual expenses incurred were well within budget.

My office consists of full-time staff, several subject-matter experts whom I engage on a part-time basis, and an independent legal counsel. I benefit from this arrangement, which allows me to bring on board people whose backgrounds are well-suited to conducting specialized work in an evolving and technically challenging field.

Resource requirements for the coming year are under review, given additional responsibilities conferred on the Commissioner through amendments to the *National Defence Act* and the *Security of Information Act*.

Commissioner's reappointment

Although the position of Commissioner of the Communications Security Establishment is now established in law, the appointment of the individual to fill the office is still made by the Governor in Council for a specified term. My current appointment is for a three-year term that expires in June 2002, and I have been reappointed for a further year to June 2003.

Review agencies conference

The third international Review Agencies Conference was scheduled to take place in Washington, D.C., in mid-October 2001, following on conferences in Canberra (1997) and Ottawa (1999). Following the events of September 11, the Washington conference was cancelled. My colleagues and I convened in London, England, May 12-14, 2002, to exchange knowledge and experiences and to renew acquaintanceships.

LOOKING AHEAD

Safeguarding the privacy of Canadians

Last year, I concluded my report by observing that CSE must constantly progress to keep pace with technological advances. Only by doing this can CSE improve its ability to screen out Canadian communications and safeguard the privacy of Canadians.

Despite the enormity of events since my last report and the pressures now on Canada's security and intelligence community to provide information and produce results, to my mind the issue of privacy remains paramount.

CSE's additional powers under Ministerial authorization are new and important tools in the fight against terrorism. At the same time, however, they must be used judiciously and in a manner consistent with the letter and the spirit of the law. This will require conscientious effort on the part of all parties as we establish and implement appropriate procedures to discharge our legislated duties.

I am also well aware of the challenges these new powers present for the review of CSE's activities. I intend to fulfil my responsibilities in the year ahead vigilantly, with this fact firmly in mind.



CANADA

PRIVY COUNCIL • CONSEIL PRIVÉ

P.C. 1999-1048
June 8, 1999

His Excellency the Governor General in Council, on the recommendation of the Minister of National Defence, pursuant to Part II of the *Inquiries Act*, hereby authorizes the Minister of National Defence (in this order referred to as "the Minister")

(a) to re-appoint the Honourable Claude Bisson of Montreal, Quebec, for a period of three years, as a commissioner ("the Commissioner") to review the activities of the Communications Security Establishment ("CSE") for the purpose of determining whether those activities are in compliance with the law;

(b) to authorize the Commissioner to commence that review on his own initiative or at the request of the Minister;

(c) to authorize the Commissioner to investigate any complaint, concerning the lawfulness of CSE activities, made by any individual who is a Canadian citizen or a permanent resident of Canada;

(d) to authorize the Commissioner not to investigate complaints for which, in the Commissioner's opinion, other avenues of redress are established by statute;

(e) to specifically authorize the Commissioner to inform any complainant of the results of his investigation, ensuring that no classified information is disclosed to the complainant;

(f) to direct the Commissioner to inform the Minister and the Attorney General of Canada of any CSE activity that the Commissioner believes may not be in compliance with the law;

.../2

- 2 -

(g) to direct the Commissioner to submit to the Minister, once each year and in both official languages, a report on the Commissioner's activities and findings that are not classified, which report the Minister will table in Parliament;

(h) to authorize the Commissioner, at any time the Commissioner considers it advisable, to submit a report containing classified information to the Minister;

(i) to direct the Commissioner, before submitting any report to the Minister, to consult with the Deputy Secretary to the Cabinet (Security and Intelligence) at the Privy Council Office for the purpose of ensuring compliance with all security requirements and the preservation of the secrecy of sources of security and intelligence information and of the security of information provided to Canada in confidence by other nations;

(j) to direct the Commissioner and all persons engaged on his behalf take an oath of secrecy and comply with all applicable government security requirements;

(k) to authorize the Commissioner to engage the services of any staff, advisors and counsel that he considers necessary to assist him in the performance of his duties and functions at such rates of remuneration and reimbursement as may be approved by the Treasury Board;

.../3

- 3 -

(l) to fix the remuneration of the Commissioner at the per diem rate set out in the annexed schedule, which rate is within the range of \$400 to \$500; and

(m) to authorize that the Commissioner be paid reasonable travel and living expenses incurred by him in the performance of his duties and functions while absent from his ordinary place of residence, in accordance with Treasury Board travel directives;

effective June 19, 1999.

CERTIFIED TO BE A TRUE COPY—COPIE CERTIFIÉE CONFORME



CLERK OF THE PRIVY COUNCIL—LE GREFFIER DU CONSEIL PRIVÉ

Classified Reports, 1996-2002

Classified Report to the Minister - March 3, 1997 (TOP SECRET)

Classified Report to the Minister

- Operational Policies with Lawfulness Implications - February 6, 1998 (SECRET)

Classified Report to the Minister

- CSE's Activities under *** - March 5, 1998 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- Internal Investigations and Complaints - March 10, 1998 (SECRET)

Classified Report to the Minister

- CSE's activities under *** - December 10, 1998 (TOP SECRET/CEO)

Classified Report to the Minister

- On controlling communications security (COMSEC) material - May 6, 1999 (TOP SECRET)

Classified Report to the Minister

- How We Test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) - June 14, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- A Study of the *** Collection Program - November 19, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- On *** - December 8, 1999 (TOP SECRET - COMINT)

Classified Report to the Minister

- A Study of the *** Reporting Process - an overview (Phase I) - December 8, 1999 (SECRET/CEO)

Classified Report to the Minister

- A Study of Selection and *** - an overview - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- CSE's Operational Support Activities Under *** - follow-up - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- Internal Investigations and Complaints - follow-up - May 10, 2000 (SECRET)

Classified Report to the Minister

- On findings of an external review of CSE's ITS Program - June 15, 2000 (SECRET)

Classified Report to the Minister

- CSE's Policy System Review - September 14, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- A study of the *** Reporting Process - Phase II *** - April 6, 2001 (SECRET/CEO)

Classified Report to the Minister

- A study of the *** Reporting Process - Phase III *** - April 6, 2001 (SECRET/CEO)

Classified Report to the Minister

- CSE's participation *** - August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister

- CSE's support to ***, as authorized by *** and *** - August 20, 2001 (TOP SECRET/CEO)

- Classified Report to the Minister
- CSE's Operational Support Activities Under *** - follow-up - 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- Internal Investigations and Complaints - follow-up - 10 mai 2000 (SECRET)
- Classified Report to the Minister
- On findings of an external review of CSE's ITS Program - 15 juin 2000 (SECRET)
- Classified Report to the Minister
- CSE's Policy System Review - 14 septembre 2000 (TRÈS SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- A study of the *** Reporting Process - Phase II *** - 6 avril 2001 (SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- A study of the *** Reporting Process - Phase III *** - 6 avril 2001 (SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- CSE's participation *** - 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- CSE's support to ***, as authorized by *** and *** - 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

Rapports classifiés, 1996-2002

Classified Report to the Minister - 3 mars 1997 (TRÈS SECRET)

Classified Report to the Minister
- Operational Policies with Lawfulness Implications - 6 février 1998 (SECRET)

Classified Report to the Minister
- CSE's Activities under *** - 5 mars 1998 (TRÈS SECRET Mot
codé/Réserve aux Canadiens)

Classified Report to the Minister
- Internal Investigations and Complaints - 10 mars 1998 (SECRET)

Classified Report to the Minister
- CSE's activities under *** - 10 décembre 1998 (TRÈS SECRET/Réserve aux
Canadiens)

Classified Report to the Minister
- On controlling communications security (COMSEC) material - 6 mai 1999 (TRÈS SECRET)

Classified Report to the Minister
- How We Test (Rapport classifié sur la mise à l'essai des pratiques du CST en
matière de collecte et de conservation de renseignements électromagnétiques,
et évaluation des efforts de l'organisme pour sauvegarder la vie privée des
Canadiens) - 14 juin 1999 (TRÈS SECRET Mot codé/Réserve aux Canadiens)

Classified Report to the Minister
- A Study of the *** Collection Program - 19 novembre 1999 (TRÈS SECRET
Mot codé/Réserve aux Canadiens)

Classified Report to the Minister
- On *** - 8 décembre 1999 (TRÈS SECRET - COMINT)

Classified Report to the Minister
- A Study of the *** Reporting Process - an overview (Phase I) - 8 décembre
1999 (SECRET/Réserve aux Canadiens)

Classified Report to the Minister
- A Study of Selection and *** - an overview - 10 mai 2000 (TRÈS
SECRET/Réserve aux Canadiens)

CLERK OF THE PRIVY COUNCIL-LE GREFFIER DU CONSEIL PRIVE



CERTIFIED TO BE A TRUE COPY-COPIE CERTIFIÉE CONFORME

à compter du 19 juin 1999.

1) à fixer la rémunération du commissaire au
taux journalier établi dans l'annexe
ci-jointe, lequel se situe entre 400 \$ et 500 \$;
(m) à autoriser le remboursement des frais de
transport et de séjour raisonnables engagés
par le commissaire lorsque l'exercice de ses
fonctions l'amène à s'éloigner de son lieu de
résidence habituel, conformément aux
directives du Conseil du Trésor concernant
les déplacements;

- 3 -

.../3

k) à autoriser le commissaire à retenir les services de toute personne dont il juge avoir besoin pour l'assister dans ses fonctions, aux taux de rémunération et d'indemnisation que peut approuver le Conseil du Trésor;

j) à exiger que le commissaire et toutes les personnes engagées pour son compte prononcent un serment de discrétion et se conforment à toutes les exigences du gouvernement en matière de sécurité;

i) à enjoindre au commissaire, avant la présentation de tout rapport au ministre, de consulter le sous-secrétaire du Cabinet (Sécurité et renseignements) au Bureau du Conseil privé pour s'assurer que toutes les exigences relatives à la sécurité sont respectées, y compris la confidentialité des sources et la protection des renseignements obtenus de pays étrangers;

h) à autoriser le commissaire à présenter au ministre, et ce à tout moment jugé opportun par le commissaire, un rapport contenant des renseignements confidentiels;

g) à enjoindre au commissaire de présenter au ministre, une fois l'an et dans les deux langues officielles, un rapport sur ses activités et ses constatations qui ne sont pas de nature confidentielle, le rapport devant être déposé par le ministre au Parlement;

.../2

f) à enjoindre au commissaire de signaler au ministre et au procureur général du Canada toute activité du CST qu'il estime ne pas être conforme à la loi;

g) à autoriser expressément le commissaire à informer toute personne ayant déposé une plainte des résultats de l'enquête qui a été effectuée, en prenant soin de ne divulguer aucun renseignement confidentiel à cette personne;

d) à autoriser le commissaire à ne pas instruire une plainte lorsque, de l'avis de celui-ci, il existe d'autres recours légaux;

c) à autoriser le commissaire à instruire toute plainte concernant la légalité des activités du CST que pourrait déposer un citoyen canadien ou un résident permanent du Canada;

b) à autoriser le commissaire à entreprendre cet examen de sa propre initiative ou à la requête du ministre;

a) à reconduire l'honorable Claude Bisson, de Montréal (Québec), dans ses fonctions de commissaire du Centre de la sécurité des télécommunications (le « CST ») pour une période de trois ans pendant laquelle il examinera les activités du CST et s'assurera qu'elles sont conformes à la loi;

Sur recommandation du ministre de la Défense nationale et en vertu de la partie II de la Loi sur les enquêtes, Son Excellence le Gouverneur général en conseil autorise le ministre de la Défense nationale (le « ministre ») :

PRIVY COUNCIL • CONSEIL PRIVÉ

CANADA



C.P. 1999-1048
8 juin 1999

La troisième conférence internationale des organismes d'examen devait se tenir à Washington (D.C.) à la mi-octobre 2001, les deux premières ayant eu lieu à Canberrra (1997) et à Ottawa (1999). À la suite des événements du 11 septembre, la conférence de Washington a été annulée. Mes collègues et moi-même nous sommes réunis à Londres, du 12 au 14 mai 2002, pour discuter de nos connaissances et de nos expériences et renouer nos liens.

L'année dernière, je faisais remarquer dans la conclusion de mon rapport que le CST doit progresser constamment pour suivre le rythme de l'évolution technologique. C'est à cette condition seulement qu'il pourra améliorer ses moyens de ne pas intercepter les communications canadiennes et de protéger la vie privée des Canadiens. À mon sens, malgré l'énormité des événements survenus depuis mon dernier rapport et les pressions auxquelles est maintenant soumise la communauté canadienne de la sécurité et du renseignement afin de fournir de l'information et de produire des résultats, la question de la vie privée reste primordiale.

Les pouvoirs additionnels conférés au CST en vertu des autorisations ministérielles sont des outils nouveaux et importants dans la lutte contre le terrorisme. Cependant ils doivent faire l'objet d'une utilisation judicieuse qui soit compatible avec la lettre et l'esprit de la loi. Toutes les parties devront faire preuve de diligence, alors que nous établirons et appliquerons les procédures voulues pour nous acquitter des responsabilités que nous confère la loi. Je suis également conscient des défis que ces nouveaux pouvoirs présentent pour l'examen des activités du CST. J'entends exercer mes responsabilités avec vigilance au cours de l'année à venir, en ayant cette réalité bien présente à l'esprit.

Renouvellement du mandat du commissaire

Budget et personnel

En ce qui me concerne, un amendement à la *Loi sur la défense nationale* me conférerait, en tant que commissaire du CST, une nouvelle responsabilité d'examen des activités entreprises par le ministère de la Défense nationale ou par les Forces canadiennes pour protéger leurs réseaux et systèmes informatiques.

Au cours des prochains mois, je compte me pencher sur cette nouvelle disposition et sur son incidence éventuelle sur mon bureau.

Au cours de l'année financière 2001-2002, j'ai disposé d'un budget de 647 150 \$. Les dépenses engagées par mon bureau sont restées en deçà des limites de ce budget.

Mon bureau comprend des employés à plein temps, plusieurs spécialistes de questions particulières, dont je retiens les services à temps partiel, et un conseiller juridique indépendant. Je trouve cette formule avantageuse, car elle me permet de faire appel à des personnes possédant une formation et une expérience bien adaptées à l'exécution de travaux spécialisés dans un domaine en évolution et exigeant sur le plan technique.

Les besoins de ressources pour l'année à venir sont à l'étude, étant donné les responsabilités additionnelles confiées au commissaire par suite des modifications apportées à la *Loi sur la défense nationale* et à la

Loi sur la protection de l'information.

Même si le poste de commissaire du Centre de la sécurité des télécommunications est maintenant établi dans la loi, la personne appelée à le remplir est toujours nommée par le gouverneur en conseil pour une période déterminée. Mon mandat actuel porte sur une période de trois ans qui prend fin en juin 2002; il a été prolongé d'un an, soit jusqu'en juin 2003.

Mon mandat m'autorise à présenter des rapports classifiés au ministre au sujet des activités du CST. Depuis ma nomination, en 1996, j'ai présenté 19 rapports de cette nature, dont deux en 2001-2002. En outre, deux autres rapports étaient presque achevés à la fin de l'année. Les enquêtes que j'ai effectuées pour rédiger ces rapports n'ont révélé aucune preuve d'activité illégale de la part du CST. On trouvera à l'annexe B la liste complète des rapports classifiés que j'ai présentés au ministre.

Au cours de l'année 2001-2002, j'ai reçu une plainte d'un membre du public au sujet du CST. J'ai examiné celle-ci et déterminé qu'aucune autre mesure n'était nécessaire.

Chaque année, je rends compte dans ce rapport de mes constatations touchant la légalité des activités du CST en me fondant sur les résultats d'une série d'examen. Ceux-ci comprennent, entre autres, une étude des autorisations juridiques en vertu desquelles le CST exerce ses activités ainsi que de ses politiques et procédures connexes.

Je suis en mesure d'affirmer que les activités du CST examinées au cours de la période visée ont été conformes à la loi et à la politique en vigueur. Je n'ai par ailleurs relevé aucune preuve indiquant que le CST aurait ciblé les communications de Canadiens ou de résidents permanents du Canada.

En avril 2002, le gouvernement a introduit le projet de loi C-55, intitulé *Loi sur la sécurité publique*. Cette mesure législative, qui est encore à l'étude au Parlement, est complémentaire à la *Loi antiterroriste* qui a été adoptée en décembre 2001. Les amendements proposés par le projet de loi C-55 touchent un grand nombre de sujets, de la sécurité des transports à l'immigration en passant par les armes biologiques.

Rapports classifiés

Plaintes

Constatations relatives à l'année 2001-2002

L'ANNÉE À VENIR La Loi sur la sécurité publique

ACTIVITÉS DE L'ANNÉE 2001-2002 La Loi antiterroriste

qu'institution gouvernementale permanente souleve une multitude de questions administratives pratiques qu'il faudra résoudre. En premier lieu, je devrai m'assurer que mon bureau dispose de ressources suffisantes pour examiner les activités élargies du CST. En outre, au cours des mois à venir, il faudra examiner d'autres questions, comme celle de la place de mon bureau au sein du gouvernement.

Lorsque les parlementaires ont étudié la *Loi antiterroriste*, l'automne dernier, ils ont sollicité mon avis sur les parties de cette mesure législative qui traitent du CST et du commissaire du CST. En octobre 2001, j'ai comparu devant le Comité sénatorial spécial chargé de l'étude du projet de loi C-36 et, en novembre, j'ai présenté un mémoire au Comité permanent de la Chambre des communes sur la justice et les droits de la personne. Le texte de mon allocution d'ouverture devant le Comité du Sénat et celui de mon mémoire au Comité de la Chambre sont affichés sur le site Web de mon bureau, à l'adresse <http://csec-ccst.gc.ca>.

Depuis l'adoption de la *Loi*, mon personnel et moi-même nous sommes concentrés sur mes nouvelles responsabilités. Le fait le plus marquant a été, au début de 2002, la mise en train des préparatifs nécessaires pour entreprendre mon premier examen des activités exercées par le CST en vertu d'autorisations ministérielles délivrées par le ministre de la Défense nationale. Je ferai rapport des résultats de cet examen au ministre dans le courant de l'année. Entre le moment où la *Loi* a été adoptée et la fin de l'année financière 2001-2002, personne n'a invoqué, dans une demande relative aux activités du CST, le mécanisme de défense de l'intérêt public, établi en vertu de la *Loi sur la protection de l'information* se rapportant à la divulgation de renseignements opérationnels spéciaux.

renseignements opérationnels spéciaux. Si une personne qui s'inquiète au sujet des activités du CST ne reçoit pas de réponse de l'administrateur général ou du sous-procureur général dans un délai raisonnable, elle doit alors signaler son inquiétude au commissaire du CST et lui donner un délai raisonnable pour répondre, à défaut de quoi elle ne pourra se prévaloir de la défense d'intérêt public.

Il faudra un certain temps pour évaluer complètement les conséquences de la *Loi antiterroriste* sur mon travail. La responsabilité d'examiner les activités entreprises par le CST en vertu d'autorisations ministérielles est considérable. Ces autorisations étendront les activités du CST à de nouveaux domaines et, lorsqu'il donnera suite à cet élargissement de son mandat, je compte veiller à ce que l'organisme soit doté de politiques et de procédures appropriées, et qu'il les applique, afin de protéger la vie privée des Canadiens.

Le rôle du commissaire dans les causes faisant intervenir la défense de l'intérêt public est à certains égards comparable à la responsabilité que j'assume depuis le début à l'égard des plaintes relatives au CST, et je prévois que les mesures dont je dispose pour traiter celles-ci me permettront de réagir rapidement et de façon adéquate à toute préoccupation soulevée au sujet des activités exercées par le CST en vertu de la *Loi sur la protection de l'information*. Très peu de plaintes m'ont été présentées depuis que j'ai pris mes fonctions, en 1996. Il reste à voir si les nouvelles dispositions concernant la défense de l'intérêt public engendreront une activité additionnelle.

Le mandat du commissaire étant maintenant clairement établi par la loi, je n'aurai plus à débattre les mérites théoriques d'un régime d'examen du CST par rapport à un autre. Toutefois, le nouveau statut du commissaire en tant

Défense d'intérêt public

- b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;
- c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

Ainsi, le mandat que je remplis depuis 1996 en vertu d'un décret est maintenant inscrit dans la loi.

La *Loi antiterroriste* a également apporté des modifications importantes à l'ancienne *Loi sur les secrets officiels*, qui s'intitule maintenant *Loi sur la protection de l'information*. Cette loi interdit désormais aux personnes astreintes au secret de communiquer ou de confirmer des « renseignements opérationnels spéciaux », ceux-ci comprenant, par définition, les renseignements relatifs aux genres d'activités qu'exerce légalement le CST.

Toutefois, une personne qui pourrait établir qu'elle a agi dans l'intérêt public en communiquant ou en confirmant des renseignements opérationnels spéciaux ne serait pas coupable d'une infraction à cette partie de la *Loi*. Celle-ci prévoit qu'une personne agit dans l'intérêt public si son but est de révéler « qu'une infraction à une loi fédérale a été, est en train ou est sur le point d'être commise par une personne dans l'exercice effectif ou censé tel de ses fonctions pour le compte du gouvernement fédéral ». L'intérêt public à ce que les renseignements soient divulgués doit l'emporter sur l'intérêt public à ce qu'ils ne le soient pas. D'où l'expression « défense d'intérêt public ».

Un juge ou un tribunal peut prendre en considération la défense de l'intérêt public seulement si la personne en cause a porté ses préoccupations à l'attention de l'administrateur général de l'institution concernée ou du sous-procureur général du Canada avant de divulguer les

Le mandat du commissaire

Le paragraphe 273.65(4) de la *Loi sur la défense nationale* énonce les conditions d'une telle autorisation :

- a) l'interception est nécessaire pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada;
- b) les renseignements à obtenir ne peuvent raisonnablement être obtenus d'une autre manière;
- c) le consentement des personnes dont les communications peuvent être interceptées ne peut raisonnablement être obtenu;
- d) des mesures satisfaisantes sont en place pour faire en sorte que seuls les renseignements qui sont essentiels pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada seront utilisés ou conservés;
- e) des mesures satisfaisantes sont en place pour protéger la vie privée des Canadiens en ce qui touche l'utilisation et la conservation de ces renseignements.

La *Loi* prévoit que le commissaire du CST doit faire enquête sur les activités exercées en vertu d'autorisations ministérielles pour en contrôler la conformité, et rendre compte de ses enquêtes annuellement au ministre.

En plus d'assigner au commissaire la responsabilité de faire enquête sur les activités exercées par le CST en vertu d'autorisations ministérielles, la *Loi sur la défense nationale* lui confie le mandat :

- a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

moyen d'une autorisation ministérielle écrite. Ainsi, le ministre peut délivrer cette autorisation, à la seule fin d'obtenir des renseignements étrangers, s'il est convaincu que les conditions suivantes sont réunies :

- a) l'interception vise des entités étrangères situées à l'extérieur du Canada;
- b) les renseignements à obtenir ne peuvent raisonnablement être obtenus d'une autre manière;
- c) la valeur des renseignements étrangers que l'on espère obtenir grâce à l'interception justifie l'interception envisagée;
- d) il existe des mesures satisfaisantes pour protéger la vie privée des Canadiens et pour faire en sorte que les communications privées ne seront utilisées ou conservées que si elles sont essentielles aux affaires internationales, à la défense ou à la sécurité.

Par le passé, il était interdit au CST d'intercepter toute communication dans laquelle l'un des participants se trouvait au Canada – même si la cible de l'interception se trouvait à l'extérieur du pays. Cette nouvelle disposition permet au ministre de la Défense nationale d'autoriser les interceptions de cette nature dans les circonstances définies dans l'autorisation. Il pourrait s'agir, par exemple, d'une communication dans laquelle une personne d'un autre pays présentant un intérêt pour le renseignement étranger communique avec un collaborateur au Canada.

La nouvelle *Loi* permet en outre au ministre de délivrer des autorisations d'intercepter des communications privées « dans le seul but de protéger les systèmes ou les réseaux informatiques du gouvernement du Canada de tout méfait ou de toute utilisation non autorisée ou de toute perturbation de leur fonctionnement ».

La Loi antiterroriste établit l'assise législative du CST en modifiant la Loi sur la défense nationale. Le nouvel article 273.64 de la Loi sur la défense nationale prévoit ce qui suit :

- (1) Le mandat du Centre de la sécurité des télécommunications est le suivant :
 - a) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;
 - b) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;
 - c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère.
 - (2) Les activités mentionnées aux alinéas (1)a) ou b)
 - a) ne peuvent viser des Canadiens ou toute personne au Canada;
 - b) doivent être soumises à des mesures de protection de la vie privée des Canadiens lors de l'utilisation et de la conservation des renseignements interceptés.
- Ces dispositions ont pour effet d'inscrire dans la loi les activités qu'exerce le CST depuis ses débuts.

La Loi sur la défense nationale dispose en outre que le ministre de la Défense nationale peut autoriser le CST à intercepter des communications privées dans des circonstances particulières, au

pratiques d'information justes. Toutefois, il recommandait lui aussi outre l'adoption d'une loi habilitante pour le CST.

Plus tard la même année, le vérificateur général du Canada déposait un rapport sur la communauté canadienne du renseignement, dans lequel il invitait le gouvernement à étudier les avantages d'un cadre législatif approprié pour le CST. Il réitéra cet avis dans un court rapport de suivi, en 1998.

De même, en 1999, le Comité sénatorial sur la sécurité et le renseignement, présidé par l'ancien sénateur William Kelly, recommandait que le CST soit fondé sur une loi qui lui soit propre et que cette loi prévoie la création d'un organisme permanent et distinct d'examen de ses activités.

Dans quatre de mes rapports annuels, j'ai soulevé la question d'un texte de loi prévoyant l'établissement du CST. Dans ces rapports et ailleurs, j'ai fait valoir que l'adoption d'une loi qui définirait le mandat et les pouvoirs du CST ainsi que ses rapports avec le Parlement, le gouvernement et le ministre de la Défense nationale constituerait une mesure appropriée conférant à l'organisme une solide assise.

Ce qui avait été débattu depuis des années s'est soudainement réalisé. Le gouvernement a accepté l'avis de ses observateurs indépendants et convenu que, dans le contexte du projet de loi omnibus C-36, le moment était venu de présenter une loi relative au CST et au commissaire de cet organisme.

Selon moi, l'adoption de cette loi est opportune. Je pense en outre qu'elle prend en compte comme il convient l'équilibre crucial qui doit exister entre la nécessité pour l'État de recueillir des renseignements afin de protéger ses citoyens et les droits individuels de ceux-ci à leur vie privée. Les parties de la Loi qui ont trait au CST et au commissaire sont décrites ci-après.

Mon rapport de cette année décrit les parties de la loi qui concernent le CST et le commissaire, et les incidences de la loi. Comme l'exige mon mandat, il rend également compte des activités de mon bureau et des constatations faites en 2001-2002.

La *Loi antiterroriste* est une mesure législative majeure dont maints éléments touchent de nombreux domaines d'activité gouvernementale. Malgré les préoccupations soulevées par la hâte avec laquelle le texte de loi a été rédigé et débattu, je suis persuadé que ses dispositions relatives au CST et au commissaire du CST ont bénéficié de discussions qui ont eu cours pendant plusieurs années au sein du gouvernement, bien avant le 11 septembre.

LA LOI ANTITERRORISTE

Plus d'une décennie de débats

Dès 1990, le Comité spécial de la Chambre des communes sur l'examen de la *Loi sur le service canadien du renseignement de sécurité* et de la *Loi sur les infractions en matière de sécurité* avait recommandé que le Parlement établisse le CST par voie législative. À l'époque, le gouvernement avait choisi de ne pas donner suite à cette recommandation, mais il avait indiqué qu'il envisageait de donner au ministre de la Défense nationale des moyens additionnels d'examiner les activités du CST. Cela a finalement abouti à ma nomination comme premier commissaire du CST, en 1996.

La question de l'établissement du CST au moyen d'une loi a refait surface en 1996, lorsque le commissaire à la protection de la vie privée a achevé son examen de cet organisme. Il concluait que, dans la mesure où sa vérification permettait de l'établir, le CST exerçait ses activités en conformité avec la *Loi sur la protection des renseignements personnels* et avec les principes régissant des

Immédiatement après les événements du 11 septembre, les employés du CST ont travaillé jour et nuit et participé aux efforts déployés à l'échelle de la planète pour identifier les responsables des attentats perpétrés aux États-Unis et prévenir d'autres attentats. Le CST a formé, avec les autres membres de la communauté canadienne de la sécurité et du renseignement, de nouveaux partenariats dans le but commun de lutter contre la menace terroriste.

Le Gouvernement du Canada a promptement réaffirmé que le terrorisme était un sujet de préoccupation national qui touchait la sécurité du pays. Prenant acte du fait que « le terrorisme déborde les frontières et dispose de moyens perfectionnés, de sorte que son éradication pose un défi et suppose une collaboration accrue entre les États et l'accroissement de la capacité du Canada de réprimer, de détecter et de désamorcer les activités terroristes¹ », il a présenté au Parlement, en octobre dernier, son projet de loi omnibus C-36, intitulé *Loi antiterroriste*².

Ce projet de loi proposait plusieurs amendements aux lois existantes, permettant de renforcer la capacité du Canada à combattre le terrorisme et de réagir aux menaces qu'il fait planer sur la vie et les intérêts des Canadiens. Les amendements proposés qui m'intéressaient plus particulièrement visaient la *Loi sur les secrets officiels* et la *Loi sur la défense nationale*, cette dernière fournissant le fondement législatif des activités du CST et du rôle du commissaire du CST. Le projet de loi C-36, qui a été adopté par le Parlement et promulgué le 24 décembre 2001, ajoutait en outre de nouveaux éléments au rôle du CST et à celui de mon bureau.

1 Extrait du préambule du projet de loi C-36, *Loi antiterroriste*, S.C. 2001, ch. 41.

2 *Loi antiterroriste* : loi modifiant le Code criminel, la *Loi sur les secrets officiels*, la *Loi sur la preuve au Canada*, la *Loi sur le recyclage des produits de la criminalité* et d'autres lois, et édictant des mesures à l'égard de l'enregistrement des organismes de bienfaisance, en vue de combattre le terrorisme.

Depuis la publication de mon dernier rapport annuel, en mai 2001, le contexte dans lequel la communauté canadienne de la sécurité et du renseignement exerce ses activités s'est transformé. Des membres des Forces canadiennes ont participé à l'intervention militaire en Afghanistan. Notre plus proche voisin est encore en train de se remettre des attentats terroristes du 11 septembre. Les responsables des services de police et de renseignement travaillent partout au Canada ainsi qu'avec leurs homologues d'autres pays, afin de prévenir tout autre activité terroriste chez nous comme à l'étranger.

Ce nouveau contexte a amené les Canadiens à prendre davantage conscience de la façon dont le milieu de la sécurité et du renseignement, les services de police et d'incendie, les responsables de l'application des lois et les forces militaires contribuent à notre bien-être. Les Canadiens comptent sur eux pour déceler les menaces à la sécurité publique et pour arrêter ceux qui cherchent à nuire, à nous ou à nos alliés.

L'organisme dont j'examine les activités – le Centre de la sécurité des télécommunications (CST) – s'est joint à d'autres services de sécurité et de renseignement pour réagir aux événements de ces neuf derniers mois. Le CST fournit au gouvernement des renseignements étrangers en recueillant et en analysant de l'information comme des transmissions électroniques et des données qu'il tire de l'infrastructure d'information mondiale (renseignement électromagnétique), et en communiquant des rapports à ce sujet. Il contribue en outre à faire en sorte que l'information électronique du gouvernement canadien et son infrastructure soient protégées contre l'interception, la perturbation, la manipulation et le sabotage (sécurité des technologies de l'information).

TABLe DES MATIÈRES

1	Introduction
3	La Loi antiterroriste.....
3	• Plus d'une décennie de débats
5	• Le mandat du Centre de la sécurité des télécommunications.....
5	• Autorisation ministérielle
7	• Le mandat du commissaire
8	• Défense d'intérêt public
9	• Conséquences pour le commissaire
10	Activités de l'année 2001-2002.....
10	• La Loi antiterroriste.....
10	• Rapports classifiés
11	• Plaintes.....
11	• Constatations relatives à l'année 2001-2002
11	L'année à venir
11	• La Loi sur la sécurité publique
11	• Budget et personnel
12	• Renouvellement du mandat du commissaire
12	• Conférence des organismes d'examen.....
13	Coup d'œil sur l'avenir.....
13	• Protéger la vie privée des Canadiens
15	Annexe A: Mandat du commissaire
19	Annexe B: Rapports classifiés, 1996-2002

Commissaire du Centre de la
sécurité des télécommunications



Communications Security
Establishment Commissioner
The Honourable Claude Bisson, O.C.

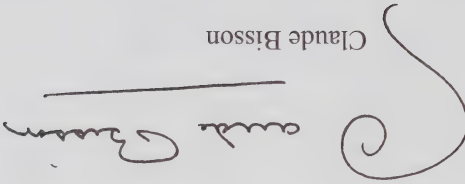
Juin 2002

L'honorable John McCallum, C.P.
Ministre de la Défense nationale
Edifice Mgen G.R. Parkes, 13e étage
101, promenade Colonel By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63 (3) de la *Loi sur la défense nationale*, j'ai le plaisir de vous soumettre mon rapport annuel pour l'année 2001-2002, qui fait état de mes activités et constatations, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.


Claude Bisson

Bureau du Commissaire du Centre de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044

Télex : (613) 992-4096

© Ministre des Travaux publics et des Services gouvernementaux Canada 2002
ISBN 0-662-66619-4
N° de cat. D95-2002

Commissaire
du Centre
de la sécurité
des télécommunications

Rapport annuel



2001
↑
2002



Canada

CA1
ND800
-S16

Government
Publications

Communications
Security
Establishment
Commissioner

Annual Report

2002
↓
2003



Canada

Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station 'B'
Ottawa, Ontario
K1P 5R5

Tel: (613) 992-3044
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 2003
ISBN 0-662-67417-0
Cat. No. D95-2003

Communications Security
Establishment Commissioner



The Honourable Claude Bisson, O.C.

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Claude Bisson, O.C.

June 2003

The Honourable John McCallum, P.C.
Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Mr. McCallum:

Pursuant to sub-section 273.63 (3) of the *National Defence Act*, I am pleased to submit to you my 2002-2003 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

A handwritten signature in dark ink, appearing to read "Claude Bisson". The signature is written in a cursive style. Below the signature is a horizontal line.

Claude Bisson

TABLE OF CONTENTS

Introduction	1
The Evolving Role of the Commissioner	2
2002-2003 Activities	4
• Classified Reports	4
• Reviews of Activities under Ministerial Authorizations	5
• Other Reviews.....	7
• 2002-03 Findings	9
• Complaints and Concerns about CSE Activities	10
• Review Agencies Conference	10
The Commissioner's Office.....	11
• Office Expenditures and Staff.....	11
• Accommodation.....	11
Looking Ahead	11
• The Public Safety Act	11
• Appointment of a New Commissioner	12
• Concluding Thoughts.....	13
Annex A: Commissioner's Mandate	15
Annex B: Budget and Expenditures 2002-03.....	17
Annex C: Classified Reports, 1996-2003	19

INTRODUCTION

This is my seventh and final report as Commissioner of the Communications Security Establishment (CSE), as my appointment will terminate in June 2003. It is also the first time since my initial appointment in 1996 that my review of CSE's activities and my annual report have been guided by legislation.

In my last report I pointed out that after more than a decade of debate about the pros and cons of enabling legislation for CSE, the tragic events of 11 September 2001 precipitated the introduction and passage of the omnibus *Anti-Terrorism Act* by Parliament. The resulting amendments to the *National Defence Act*, which came into effect on 24 December 2001, created a legislated mandate for CSE as well as for the CSE Commissioner. The new provisions of the *National Defence Act* enshrined in legislation the historical activities of CSE as well as the activities I had been carrying out since 1996, but they also introduced new elements. These are described more fully in the next section.

Much of this past year has been taken up with assessing the implications of my new duties and making a start on meeting the requirements of the legislation. As a result, it has been a year of much challenge and change for both CSE and my Office as we move toward a common understanding of our respective roles and responsibilities.

In this year's annual report I look back briefly on seven years of evolution and development in the Commissioner's role. I also report on the review activities and findings of my Office in 2002-03. These addressed CSE's two main programs (Signals Intelligence and Information Technology Security) as well as some of its other activities. Finally, I look forward to developments that are already on the horizon and to the appointment of my successor.

THE EVOLVING ROLE OF THE COMMISSIONER

Since I started as Commissioner in 1996, the highly complex environment in which CSE works has changed dramatically. So has the work of my Office and the expectations placed upon it.

One aspect of the change results from the technology-rich environment within which CSE works – and the technology involved has been advancing at an accelerating pace throughout this time. Another key element relates to changes in the intelligence environment that derive from evolving political, social and economic realities. These have led to new threats to Canada's security, defence and national interests and changes to the government's intelligence priorities. To address these challenges, CSE has expanded its role in the collection, analysis and reporting of information and intelligence. My staff and I have had to learn about the complex technologies involved and to stay on top of the rapid changes taking place in order to carry out the Commissioner's review role effectively and efficiently.

Throughout this period of dynamic change in technology, in the intelligence environment, and in CSE's activities, I have been guided by the principle that Canadians deserve the assurance that CSE, which must of necessity conduct most of its business in secret, does so in compliance with the laws of Canada. Providing this assurance has been my responsibility, and I have sought to fulfil it by maintaining the breadth, depth and credibility of my Office's review work, with a particular focus on those matters that could put the privacy of Canadians at risk.

The Commissioner's role, as it had developed under mandates set out in the June 1996 and June 1999 Orders in Council appointing me Commissioner, was confirmed and extended by Parliament in the *Anti-Terrorism Act* of December 2001. The most significant extension of my role arises from

provisions that allow the Minister of National Defence to authorize CSE's interception of the private communications of Canadians in specific circumstances and subject to several conditions set out in the legislation.¹ Section 183 of the *Criminal Code* defines private communications as

...any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada, and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it...

This new power of CSE to intercept private communications when authorized by the Minister is a significant development, bringing with it obvious risks to the privacy of Canadians. These risks are recognized in the legislation, which requires, among other things, that the Minister be satisfied that CSE has satisfactory measures in place to protect the privacy of Canadians. In addition, the legislation directs the Commissioner to review activities carried out under each ministerial authorization to ensure that they are indeed authorized, and to report annually to the Minister on the review. Based on experience to date, I anticipate that this will be a substantial and challenging aspect of the Commissioner's role in the future.

A further extension to the Commissioner's role was set out in the *Security of Information Act* (the former *Official Secrets Act*). This Act prohibits people bound by secrecy from communicating or confirming "special operational information", including special operational information about

¹ Before December 2001, CSE would have been in violation of privacy-related provisions of both the *Criminal Code* and the *Canadian Charter of Rights and Freedoms* had it intercepted communications without the certainty that, in doing so, it would not intercept private communications.

CSE's activities. A person would not be found guilty of an offence, however, if that person could establish that he or she acted in the public interest. A judge can consider a "public interest defence" only if the person involved has taken a series of steps set out in the legislation before disclosing the information. These steps may include bringing concerns about CSE's activities to the Commissioner and allowing a reasonable time for the Commissioner to respond. Although I am hopeful that this role will rarely be exercised, it is potentially an important one and is likely to be demanding when a concern is brought to the Commissioner's attention.

The legislative provisions setting out the mandate of the Commissioner of the Communications Security Establishment are included in Annex A.

2002-03 ACTIVITIES Classified Reports

Under the Orders in Council that set out my mandate from 19 June 1996 until 24 December 2001, my Office carried out a planned series of reviews of CSE's activities each year. These reviews were directed at areas where, in my opinion, the very nature of CSE's activities gave rise to risks relating to lawfulness. Because I was authorized to submit reports containing classified material to the Minister of National Defence at any time I considered advisable, I made it a practice to report the results of each of my reviews to the Minister in the form of a classified report.

The new legislation has introduced some important changes to my mandate. As described above, the Minister of National Defence may now authorize CSE to intercept the private communications of Canadians in some circumstances. Although I am still required to review CSE's activities generally to ensure that they are in compliance with the law, the legislation also directs me specifically to review CSE activities carried out under a ministerial

authorization to ensure they are authorized, and to report annually to the Minister on the review.

In other words, I no longer have a completely free hand in choosing subjects for review. Nor does my new legislated mandate specifically authorize me to submit reports containing classified material to the Minister whenever I consider it advisable. Nevertheless, in cases where I do choose the subjects for review, I believe it is sensible to continue the reporting practices established under my earlier mandate, as they have served well in the past.

During 2002-03 I forwarded four classified reports to the Minister, and another was nearing completion at the end of the year. These included reports mandated under the new legislation as well as reports on reviews of my own choosing. Annex C provides a list of all my classified reports to the Minister since my appointment in 1996.

As I have pointed out in the past, submitting a classified report to the Minister does not mean that I have identified any lack of compliance with the law or ministerial authority. It indicates only that the report contains material that requires classified handling. Indeed, I am pleased to say that none of the reviews on which my 23 classified reports are based (including the four reviews completed in 2002-03) identified incidents of unlawfulness or unauthorized activity.

Reviews of Activities under Ministerial Authorizations

Under sub-sections 273.65 (1) and (3) of the *National Defence Act*, the Minister of National Defence has authorized CSE, in writing, to intercept private communications for the purposes of obtaining foreign intelligence and protecting the computer systems or networks of the government from mischief, unauthorized use or interference. Because many of the activities carried out under

these authorizations were new to CSE, they gave rise to significant challenges relating not only to technology, but also to such matters as determining appropriate roles and responsibilities, developing policy and procedures to guide activities, and designing controls to ensure compliance with the conditions imposed by the legislation and the ministerial authorizations. CSE continues to address these challenges.

Information obtained from CSE indicates that the bulk of the communications intercepted under these authorizations are not in fact private communications (that is, they are not the communications of Canadians). Nevertheless, I believe that the unique focus of my review must be on private communications. Whatever else CSE may intercept, it is the interception of private communications that is specifically authorized by the Minister. Moreover, it is with respect to the interception, use and retention of private communications that issues of lawfulness and compliance with ministerial authority are most likely to arise. As a result, my Office devoted a significant part of its efforts during the past year to learning how CSE is acquiring, identifying, accessing, retaining and using such communications, as well as what kind of policy regime, procedures and management control framework it is putting in place. In doing so, my staff and I examined a variety of documents and correspondence, had several discussions with CSE officials, and attended briefings and information sessions. In addition, I asked CSE to take me through a specific tasking under one of the authorizations.

My Office completed a preliminary review of activities under one ministerial authorization. This authorized CSE to conduct activities from Canada relating to the interception of communications for the sole purpose of obtaining foreign intelligence

and, in doing so, to intercept private communications subject to conditions defined in the legislation and in the ministerial authorization. As required by the legislation, I reported the findings of this preliminary review to the Minister. Because of the focus of the ministerial authorization, and because the review was a first for my Office, my preliminary report related more to process and to the class of activities authorized than to CSE's compliance with authority. I anticipate that in future annual reports to the Minister under paragraph 273.65 of Part V.1 of the *National Defence Act*, the Commissioner will be in a position to address compliance issues more directly.

My reviews of activities under other ministerial authorizations in effect during 2002-03 were continuing at the end of the year and will be the subject of reports to the Minister in the near future.

Other Reviews

CSE's operational support to the Canadian Security Intelligence Service. The Canadian Security Intelligence Service (CSIS) is authorized to assist the ministers of National Defence and Foreign Affairs in collecting foreign intelligence within Canada. In carrying out its duties and functions, CSIS may, in turn, seek operational assistance and support from other departments and agencies, including CSE.

In 2002-03 my staff completed an examination of CSE's policies and practices in the context of a specific case where it provided operational support to CSIS. This examination found no evidence of unlawful activity on the part of CSE or any of its employees. Indeed, all the activities examined complied with CSE policies as well as relevant legal authorities.

My report did, however, make a number of recommendations designed to address weaknesses

in policy and practice that could lead to errors in handling sensitive information and to an inconsistent application of policy and law. CSE has started to take action to address the concerns I raised.

Information Technology Security. In earlier annual reports I discussed changes in the focus and complexity of activities undertaken by CSE under its Information Technology Security (ITS) program to protect government communications and communications systems. Among other things, the ITS program has shifted strategically toward a more open mode of doing business in the face of growing vulnerabilities as more and more government organizations adopt evolving technologies such as the Internet and electronic commerce.

To respond to a significantly expanded client base and greater demand for its services, the ITS program has actively sought cooperative partnerships and alliances with government and private sector organizations. These arrangements are usually formalized in written agreements between the parties. My Office reviewed formal agreements between the ITS program and external parties, as well as the policies, practices and procedures governing them, to identify issues and assess implications relating to lawfulness.

The review showed no evidence of unlawful activity on the part of CSE with respect to its arrangements with government and private sector organizations and the agreements arising from such arrangements. However, my report pointed to shortcomings in the administration of agreements as well as gaps in policy that created unnecessary risks in this regard. I have been informed that CSE is taking action to review and address my concerns and recommendations.

CSE's policies and procedures. One of my long-standing observations, based on several reviews carried out during my term as Commissioner, is that

CSE's internal policies and procedures have not always provided clear and consistent definitions and uses of key terms. I have found that policies and associated documentation were confusing at times, especially in instances where certain terms have multiple definitions.

As a follow-up to these observations, my staff compiled a lexicon of definitions of key terms from a number of different instruments, and I made that report available to the Minister and to CSE. In the course of this work, I learned that CSE is giving a high priority to the development and articulation of policies and procedures to guide operations under its mandate in the *National Defence Act*. This effort includes establishing new policies and procedures where necessary, as well as reviewing existing policies and procedures to ensure they are current and that they use accurate and consistent terminology.

I am encouraged by these developments at a time of expanded security and intelligence activity when, among other things, there are clear needs for CSE to retrain existing staff and to train and guide an anticipated influx of new employees. In these circumstances it is vitally important to ensure clear and consistent understanding and application of policy and procedures – including terminology used – throughout the organization. My Office will continue to monitor CSE's progress in this regard closely.

2002-03 Findings

Each year in this report I provide an overall statement on my findings about the lawfulness of CSE's activities based on the results of reviews my staff carried out during the year. Because of my new mandate under the *National Defence Act*, this is the first time my statement extends beyond lawfulness to compliance with ministerial authority.

I am able to report that the activities of CSE that my Office reviewed during the year complied with law and ministerial authority. In particular, while I found no evidence that CSE directed its activities at Canadians or any person in Canada, I did see evidence that CSE has measures to protect the privacy of Canadians in the use and retention of intercepted information.

Complaints and Concerns about CSE Activities

Paragraph 273.63 (2)(b) of the *National Defence Act* requires me, in response to a complaint, to undertake any investigation I consider necessary. During 2002-03, I received no complaints about CSE activities from any source.

Neither were concerns about CSE activities addressed to me under the public interest defence provisions of the *Security of Information Act*.

Review Agencies Conference

The third International Intelligence Review Agencies Conference was held in London, England, from 12-15 May 2002. Representatives of review agencies from Australia, Belgium, Canada, New Zealand, Poland, Slovakia, South Africa, and the United States met their United Kingdom counterparts to exchange views on issues of common interest in the historical setting of Lancaster House.

In addition to discussing review arrangements in our respective jurisdictions, we examined the issue of review from the perspectives of the agency being reviewed and the public, as well as in relation to changes in technology. I remain grateful to our hosts for their outstanding hospitality.

THE COMMISSIONER'S OFFICE Office Expenditures and Staff

My budget allocation for the 2002-03 fiscal year was \$921,950. Because the December 2001 amendments to the *National Defence Act* expanded my duties significantly, this allocation was 42 per cent greater than my budget in the previous year. The actual expenditures incurred in 2002-03 (see Annex B) were well within the budget.

During the year, my Office continued to consist of a small full-time staff. In addition, to help carry out my duties, I engaged the services of an independent legal counsel and several subject-matter experts on an ongoing basis.

Accommodation

My Office has occupied the same premises since my appointment in 1996, although by 1998 it was becoming evident that these premises offered insufficient accommodation for the staff and advisors I required to discharge my responsibilities. This situation became more acute following the additional responsibilities assigned to me by Parliament in late 2001.

In late 2002, I was advised that a larger office space was about to become available in the building that my Office has occupied since 1996. It was evident that this space would suit current requirements and also provide some flexibility for the future. My Office moved to its new location in May 2003.

LOOKING AHEAD The Public Safety Act

In October 2002 the government introduced Bill C-17, the *Public Safety Act*, in Parliament. This bill, which replaced the earlier Bill C-55 (which in turn had replaced Bill C-42), was still under consideration as I was writing this report. Bill C-17 proposes legislative changes on a wide range of subjects, from transportation safety and immigration to biological weapons. Among the proposed changes are amendments to the *National Defence Act* that would confer significant new

responsibilities on the Commissioner of CSE for reviewing the lawfulness and compliance with ministerial authority of activities undertaken by the Department of National Defence or the Canadian Forces to protect their computer systems and networks, and for dealing with complaints arising from such activities.

I have informed the government of my concerns regarding the role proposed for the Commissioner in this Bill and its predecessors. Those concerns centre around the difficulties I can foresee in providing meaningful assurance of lawfulness and compliance with ministerial authority. In addition, however, I believe that assuming these new and potentially complex responsibilities would raise the question of whether the Commissioner's role could be carried out effectively on a part-time basis in the future.

In the meantime I have asked my officials to undertake a preliminary assessment of the review mandate envisaged in Bill C-17 so as to identify more clearly the systems that would be involved and the size of the sample of activities that would need to be reviewed for the Commissioner to give the assurances required. This will provide my successor with better information on the nature and extent of the work involved, and the possible impacts on this Office's resource requirements, should Parliament choose to confer these new duties on the Commissioner.

Appointment of a New Commissioner

My appointment as Commissioner expires on 19 June 2003.

Paragraph 273.63 (1) of the *National Defence Act* provides that the Governor in Council may appoint either a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment. However, I am concerned that a supernumerary judge would face serious limitations in carrying out the full range of duties and responsibilities involved.

These limitations arise from the blurring of lines between the executive and legislative arms of government on the one hand, and the judiciary on the other, that would result from appointing a supernumerary judge. For example, a supernumerary judge would not be in a position to comment on proposed legislation – as I have had occasion to do from time to time. Similarly, a supernumerary judge ought not to appear as a witness before parliamentary committees. Although I am somewhat disappointed not to have been called as a witness before parliamentary committees to discuss my annual reports, as a retired judge I would at least have been able to do so.

Regardless of the Governor in Council's decision, I wish my successor well in this fascinating and challenging assignment.

Concluding Thoughts

Finally, I would like to take this opportunity to say that serving Canada and Canadians during the past seven years has been a source of great and enduring satisfaction for me. I am convinced that through the very existence of this external review function, through the assurances that I have been able to provide and the opportunities for improvement that reviews have identified, my Office has made an important contribution to strengthening the control and accountability of CSE.

I would also like to say goodbye and to thank those I have worked with for seven years. In particular, the skill, dedication and unfailing good cheer of my staff have helped me immeasurably and have guided me through some challenging times. But I am also grateful for the respect and courtesy that CSE and other government officials have consistently extended to me and my staff. Their cooperation has made our task much easier.

Mandate of the Commissioner of the Communications Security Establishment

National Defence Act - Part V.1

“**273.63** (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner’s activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

“**273.65** (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review.”

Security of Information Act

“**15.** (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest.

“**15.** (5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following:

“**15.** (5) (b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person’s possession to,

(ii) the Communications Security Establishment Commissioner, if the person’s concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person’s duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time.”

Budget and Expenditures 2002-03

Expenditures

Salaries and Wages	201,935
Transportation and Telecommunications	21,808
Information	11,378
Professional and Special Services	209,699
Rentals	157,708
Purchased Repair and Maintenance	223,737
Materials and Supplies	4,438
Acquisition of Machinery and Equipment	26,098
Other Expenditures	22
Total	\$856,823

Classified Reports, 1996-2003

Classified Report to the Minister – March 3, 1997 (TOP SECRET)

Classified Report to the Minister

- Operational Policies with Lawfulness Implications - February 6, 1998 (SECRET)

Classified Report to the Minister

- CSE's Activities under *** - March 5, 1998 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- Internal Investigations and Complaints - March 10, 1998 (SECRET)

Classified Report to the Minister

- CSE's activities under *** - December 10, 1998 (TOP SECRET/CEO)

Classified Report to the Minister

- On controlling communications security (COMSEC) material - May 6, 1999 (TOP SECRET)

Classified Report to the Minister

- How We Test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) - June 14, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- A Study of the *** Collection Program - November 19, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister

- On *** - December 8, 1999 (TOP SECRET - COMINT)

Classified Report to the Minister

- A Study of the *** Reporting Process - an overview (Phase I) - December 8, 1999 (SECRET/CEO)

Classified Report to the Minister

- A Study of Selection and *** - an overview - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- CSE's Operational Support Activities Under *** - follow-up - May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- Internal Investigations and Complaints - follow-up - May 10, 2000 (SECRET)

Classified Report to the Minister

- On findings of an external review of CSE's ITS Program - June 15, 2000 (SECRET)

Classified Report to the Minister

- CSE's Policy System Review - September 14, 2000 (TOP SECRET/CEO)

Classified Report to the Minister

- A study of the *** Reporting Process - Phase II *** - April 6, 2001 (SECRET/CEO)

Classified Report to the Minister

- A study of the *** Reporting Process - Phase III *** - April 6, 2001 (SECRET/CEO)

Classified Report to the Minister

- CSE's participation *** - August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister

- CSE's support to ***, as authorized by *** and *** - August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister

- A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) - August 21, 2002 (SECRET)

Classified Report to the Minister

- CSE's support to CSIS, as authorized by *** and code named *** - November 13, 2002 (TOP SECRET/CEO)

Classified Report to the Minister

- CSE's SIGINT activities carried out under the *** 2002 *** ministerial authorization November 27, 2002 (TOP SECRET/CEO)

Classified Report to the Minister

- LEXICON - 26 March 2003 (TOP SECRET/COMINT)

- Classified Report to the Minister
- CSE's SIGINT activities carried out under the *** 2002 *** ministerial authorization - 27 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)
 - Classified Report to the Minister
 - LEXICON - 26 mars 2003 (TRÈS SECRET/COMINT)

- Classified Report to the Minister
- CSE's Operational Support Activities Under *** - follow-up - 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- Internal Investigations and Complaints - follow-up - 10 mai 2000 (SECRET)
- Classified Report to the Minister
- On findings of an external review of CSE's ITS Program - 15 juin 2000 (SECRET)
- Classified Report to the Minister
- CSE's Policy System Review - 14 septembre 2000 (TRÈS SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- A study of the *** Reporting Process - Phase II *** - 6 avril 2001 (SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- A study of the *** Reporting Process - Phase III *** - 6 avril 2001 (SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
CSE's participation *** - 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- CSE's support to ***, as authorized by *** and *** - 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)
- Classified Report to the Minister
- A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) - 20 août 2002 (SECRET)
- Classified Report to the Minister
- CSE's support to CSIS, as authorized by *** and code named *** - 13 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

Rapports classifiés, 1996-2003

Classified Report to the Minister - 3 mars 1997 (TRÈS SECRET)

Classified Report to the Minister
- Operational Policies with Lawfulness Implications - 6 février 1998 - (SECRET)

Classified Report to the Minister
- CSE's Activities under *** - 5 mars 1998 (TRÈS SECRET Mot codé/Réserve aux Canadiens)

Classified Report to the Minister
- Internal Investigations and Complaints - 10 mars 1998 (SECRET)

Classified Report to the Minister
- CSE's activities under *** - 10 décembre 1998 (TRÈS SECRET/Réserve aux Canadiens)

Classified Report to the Minister
- On controlling communications security (COMSEC) material - 6 mai 1999 (TRÈS SECRET)

Classified Report to the Minister
- How We Test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) - 14 juin 1999 (TRÈS SECRET Mot codé/Réserve aux Canadiens)
Classified Report to the Minister
- A Study of the *** Collection Program - 19 novembre 1999 (TRÈS SECRET Mot codé/Réserve aux Canadiens)

Classified Report to the Minister
- On *** - 8 décembre 1999 (TRÈS SECRET - COMINT)

Classified Report to the Minister
- A Study of the *** Reporting Process - an overview (Phase I) - 8 décembre 1999 (SECRET/Réserve aux Canadiens)

Classified Report to the Minister
- A Study of Selection and *** - an overview - 10 mai 2000 (TRÈS SECRET/Réserve aux Canadiens)

Budget et dépenses, 2002-2003

Dépenses

Traitements et salaires	201 935
Transports et télécommunications	21 808
Information	11 378
Services professionnels et spéciaux	209 699
Location	157 708
Achat de services de réparation et d'entretien	223 737
Fournitures et approvisionnements	4 438
Acquisition de machine et de matériel	26 098
Autres charges	22
Total	856 824 \$

« 273.65 (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre. »

Loi sur la protection de l'information

« 15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public.

« 15. (5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes :

« 15. (5) (b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession :

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable. »

Mandat du commissaire du Centre de la sécurité des télécommunications

Loi sur la défense nationale - Partie V.1

« 273.63 (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

(a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

(b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

(c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

Dernières réflexions

Ces limites tiennent au fait que la nomination d'un juge surnuméraire estomperait la démarcation entre les pouvoirs exécutif et législatif, d'une part, et le pouvoir judiciaire, de l'autre. Par exemple, un juge surnuméraire ne serait pas en mesure de commenter des projets de loi, comme j'ai eu l'occasion de le faire de temps à autre. De même, il ne devrait pas comparaître devant des comités parlementaires. Si je suis quelque peu déçu de ne pas avoir été appelé à témoigner devant des comités parlementaires pour discuter de mes rapports annuels, en ma qualité de juge à la retraite, j'aurais au moins pu le faire.

Mais quelle que soit la décision du gouverneur en conseil, je souhaite à celui ou celle qui prendra la relève un franc succès dans cette mission passionnante et exigeante.

Enfin, j'aimerais profiter de l'occasion pour dire que mon travail au service du Canada et des Canadiens au cours des sept dernières années a été pour moi une source de profonde et durable satisfaction. Je suis convaincu que, grâce à l'existence même de cette fonction d'examen externe, grâce aux assurances que j'ai pu fournir et aux possibilités d'amélioration que les examens ont fait ressortir, mon bureau a fourni un apport important au renforcement du contrôle et de la responsabilité du CST.

J'aimerais par ailleurs saluer et remercier les personnes avec qui j'ai travaillé pendant sept ans. La compétence, le dévouement et la bonne humeur indéfectible de mon personnel m'ont été d'une aide inestimable et m'ont guidé dans des moments difficiles. Je suis également reconnaissant du respect et de la courtoisie que le CST et les autres fonctionnaires de l'État nous ont toujours témoignés, à mon personnel et à moi-même. Leur coopération a grandement facilité notre tâche.

réseaux informatiques, et le traitement des plaintes
découlant de ces activités.

J'ai informé le gouvernement de mes préoccupations
au sujet du rôle proposé pour le commissaire dans
ce projet de loi et ceux qui l'ont précédé. Ces
préoccupations ont trait aux difficultés que
j'entrevois lorsqu'il s'agitrait de fournir une garantie
sérieuse de légalité et de conformité à l'autorité
ministérielle. J'estime en outre que la prise en
charge de ces responsabilités nouvelles et
susceptibles d'être complexes soulèverait la question
de savoir si les fonctions du commissaire pourraient
à l'avenir être exercées à temps partiel.

Entre-temps, j'ai demandé à mes fonctionnaires de
procéder à une évaluation préliminaire du mandat
d'examen envisagé dans le projet de loi C-17, afin de
définir plus clairement les systèmes qui seraient en
cause et la taille de l'échantillon d'activités qui
devrait être examiné pour permettre au commissaire
de donner les assurances requises. Cela fournira à
mon successeur une meilleure information sur la
nature et l'ampleur du travail, et sur ses répercussions
possibles sur les ressources nécessaires au bureau du
commissaire, si le Parlement décide de lui confier ces
nouvelles fonctions.

Mon mandat à titre de commissaire expire le
19 juin 2003.

Nomination d'un nouveau commissaire

Le paragraphe 273.63 (1) de la *Loi sur la défense
nationale* prévoit que le gouverneur en conseil peut
nommer soit un juge surnuméraire, soit un juge
d'une cour supérieure à la retraite au poste de
commissaire du Centre de la sécurité des
télécommunications. Toutefois, je m'inquiète du fait
qu'un juge surnuméraire ferait face à des limites
sérieuses pour ce qui est de remplir l'ensemble des
fonctions et des responsabilités du poste.

temps. J'ai par ailleurs retenu les services d'un conseiller juridique indépendant et de plusieurs spécialistes de questions particulières sur une base régulière pour m'aider à m'acquitter de mes fonctions.

Mon bureau est situé dans les mêmes locaux depuis ma nomination, en 1996, même si, dès 1998, il est devenu évident que ceux-ci étaient insuffisants pour loger le personnel et les conseillers dont j'ai besoin pour m'acquitter de mes responsabilités. Cette situation est devenue plus critique après que le Parlement m'a confié de nouvelles responsabilités, à la fin de 2001.

À la fin de 2002, on m'a informé que des locaux plus spacieux étaient sur le point de se libérer dans l'immeuble où se trouve mon bureau depuis 1996. Il était évident que cet espace répondrait aux besoins actuels et assurerait une certaine souplesse pour l'avenir. Nous avons emménagé dans ces nouveaux locaux en mai 2003.

Locaux

COUP D'ŒIL SUR L'AVENIR La Loi sur la sécurité publique

En octobre 2002, le gouvernement a déposé au Parlement le projet de loi C-17, *Loi sur la sécurité publique*. Celui-ci, qui a remplacé le projet de loi C-55, déposé antérieurement (et qui avait lui-même remplacé le projet de loi C-42), était encore à l'étude au Parlement au moment de la rédaction du présent rapport. Le projet de loi C-17 propose des modifications législatives touchant un grand nombre de sujets, de la sécurité des transports à l'immigration en passant par les armes biologiques. Parmi celles-ci figurent des modifications de la *Loi sur la défense nationale* qui confèreraient de nouvelles responsabilités importantes au commissaire du CST touchant l'examen de la légalité et de la conformité à l'autorisation ministérielle des activités entreprises par le ministère de la Défense nationale ou par les Forces canadiennes afin de protéger leurs systèmes et

Plaintes et préoccupations relatives aux activités du CST

L'alinéa 273.63 (2)b) de la *Loi sur la défense nationale* m'oblige à effectuer toute enquête que je juge nécessaire à la suite d'une plainte. Au cours de l'année 2002-2003, je n'ai reçu aucune plainte de quelque source que ce soit au sujet des activités du CST.

On ne m'a pas non plus signalé de préoccupations au sujet des activités du CST en vertu des dispositions de la *Loi sur la protection de l'information* portant sur la défense d'intérêt public.

Conférence des organismes d'examen

La troisième conférence internationale des organismes d'examen des activités de renseignement s'est tenue à Londres, en Angleterre, du 12 au 15 mai 2002. Des représentants de l'Afrique du Sud, de l'Australie, de la Belgique, du Canada, des États-Unis, de la Nouvelle-Zélande, de la Pologne et de la Slovaquie ont rencontré leurs homologues du Royaume-Uni pour discuter de questions d'intérêt commun, dans le cadre historique de Lancaster House.

Outre les modalités d'examen dans nos pays respectifs, nous avons examiné la question de l'examen du point de vue de l'organisme visé et du public, ainsi que par rapport à l'évolution de la technologie. Je suis reconnaissant à nos hôtes de leur généreuse hospitalité.

LE BUREAU DU COMMISSAIRE Dépenses du bureau et personnel

Le budget qui m'avait été alloué pour l'année financière 2002-2003 était de 921 950 \$. Comme les modifications apportées à la *Loi sur la défense nationale* en décembre 2001 avaient sensiblement élargi mes fonctions, ce budget dépassait celui de l'année précédente de 42 p. 100. Les dépenses engagées en 2002-2003 (voir l'annexe B) sont restées bien en deçà de ce budget.

Au cours de l'année, mon bureau a continué de se composer d'un petit noyau de personnel à plein

Constatations faites en 2002-2003

politiques et de procédures destinées à guider les opérations découlant de son mandat énoncé dans la *Loi sur la défense nationale*. Cette entreprise comprend l'établissement de politiques et de procédures nouvelles, là où c'est nécessaire, ainsi que l'examen des politiques et des procédures existantes pour s'assurer qu'elles sont d'actualité et qu'elles emploient une terminologie exacte et uniforme.

Je suis encouragé par cette évolution à un moment où les activités de sécurité et de renseignement sont en plein essor et où il est évident que le CST doit assurer le perfectionnement de son personnel en place, en plus de former et de guider une future cohorte de nouveaux employés. Dans ces circonstances, il est capital d'assurer la compréhension et l'application claires et uniformes de la politique et des procédures – y compris la terminologie employée – à l'échelle de l'organisme. Mon bureau continuera de suivre de près les progrès accomplis par le CST à cet égard.

Je fournis comme chaque année dans le présent rapport un énoncé global de mes constatations au sujet de la légalité des activités du CST, en me fondant sur les résultats des examens effectués par mon personnel pendant l'année. Compte tenu de mon nouveau mandat en vertu de la *Loi sur la défense nationale*, cet énoncé va pour la première fois au-delà de la légalité pour englober la conformité à l'autorisation ministérielle.

Je suis à même de signaler que les activités du CST que mon bureau a examinées au cours de l'année étaient conformes à la loi et à l'autorisation ministérielle. Ainsi, je n'ai trouvé aucun indice révélant que les activités du CST visaient des Canadiens ou d'autres personnes au Canada, mais j'ai vu des preuves des mesures mises en place par le CST pour protéger la vie privée des Canadiens en ce qui touche l'utilisation et la conservation des renseignements interceptés.

Compte tenu d'une augmentation considérable de sa clientèle et d'un accroissement de la demande visant ses services, le programme de STI a cherché activement à former des partenariats et des alliances avec des organismes du gouvernement et du secteur privé. Ces arrangements sont habituellement officialisés par des ententes écrites entre les parties. Mon bureau a examiné les ententes officielles entre le programme de STI et des organismes externes, ainsi que les politiques, les pratiques et les procédures qui les régissent, afin de repérer d'éventuels problèmes et d'en évaluer l'incidence sous le rapport de la légalité.

Cet examen n'a révélé aucun indice d'activité illégale de la part du CST touchant ses arrangements avec des organismes du gouvernement et du secteur privé et les ententes en découlant. Toutefois, mon rapport a souligné des défauts dans l'administration des ententes ainsi que des lacunes de politique qui créent des risques inutiles à cet égard. On m'a informé que le CST prend des mesures pour étudier mes préoccupations et mes recommandations et pour y donner suite.

Politiques et procédures du CST. L'une de mes observations de longue date, qui se fonde sur plusieurs examens effectués au cours de mon mandat, est que les politiques et les procédures internes du CST n'ont pas toujours fourni des définitions et des emplois clairs et uniformes de termes clés. J'ai constaté que les politiques et la documentation connexe étaient parfois déroutantes, en particulier lorsque certains termes ont de multiples définitions.

À la suite de ces observations, mon personnel a dressé un lexique de termes clés à partir de plusieurs outils, et j'ai communiqué ce rapport au ministre et au CST. Au cours de ce travail, j'ai appris que le CST considérait comme hautement prioritaires l'élaboration et la formulation de

Soutien opérationnel apporté par le CST au Service canadien du renseignement de sécurité. Le Service canadien du renseignement de sécurité (SCRS) est autorisé à aider le ministre de la Défense nationale et le ministre des Affaires étrangères à recueillir des renseignements étrangers au Canada. Dans l'exercice de ses fonctions et responsabilités, le SCRS peut également solliciter l'aide et le soutien opérationnels d'autres ministères et organismes, dont le CST.

En 2002-2003, mon personnel a effectué un examen des politiques et pratiques du CST dans le contexte d'un cas précis où celui-ci a apporté un soutien opérationnel au SCRS. Cet examen n'a fait ressortir aucune preuve d'activité illégale de la part du CST ni d'aucun de ses employés. En effet, toutes les activités examinées étaient conformes aux politiques de l'organisme ainsi qu'aux autorisations légales pertinentes.

Mon rapport contenait cependant un certain nombre de recommandations destinées à remédier à des faiblesses de la politique et de la pratique qui pourraient entraîner des erreurs de traitement de renseignements délicats, et à un manque d'uniformité dans l'application de la politique et de la loi. Le CST a commencé à prendre des mesures pour répondre aux préoccupations que j'ai soulevées.

Sécurité des technologies de l'information. J'ai traité dans des rapports annuels antérieurs des modifications de l'objet et de la complexité des activités menées par le CST dans le cadre de son programme de sécurité des technologies de l'information (STI) afin de protéger les communications et les systèmes de communication du gouvernement. Le programme de STI s'est entre autres réorienté stratégiquement dans le sens d'une plus grande ouverture face aux vulnérabilités qui augmentent à mesure qu'un plus grand nombre d'organisations gouvernementales adoptent des technologies nouvelles comme Internet et le commerce électronique.

En conséquence, au cours de l'année écoulée, mon bureau a consacré une bonne partie de ses activités à examiner comment le CST acquiert et reconnaît ces communications, comment il y accède, comment il les conserve et les utilise, et quel genre de politique, de procédures et de cadre de contrôle de la gestion il met en place. Pour ce faire, mon personnel et moi-même avons examiné une certaine quantité de documents et de correspondance, eu plusieurs entretiens avec des représentants du CST et assisté à des briefings et des séances d'information. J'ai en outre demandé au CST de me décrire une mission précise effectuée en vertu de l'une des autorisations.

Mon bureau a effectué un examen préliminaire d'activités menées conformément à une autorisation ministérielle. En vertu de celle-ci, le CST était autorisé à mener, à partir du Canada, des activités relatives à l'interception de communications dans le seul but d'obtenir des renseignements étrangers et, ce faisant, d'intercepter des communications privées sous réserve des conditions définies dans la loi et dans l'autorisation ministérielle. Comme l'exige la loi, j'ai fait rapport au ministre des constatations issues de cet examen préliminaire. En raison de l'objet de l'autorisation ministérielle, et parce que cet examen était une première pour mon bureau, mon rapport préliminaire a porté davantage sur le processus et la classe d'activités autorisées que sur la conformité du CST à l'autorisation. Je prévois que, dans les rapports annuels futurs qu'il adressera au ministre en vertu de l'article 273.65 de la partie V.1 de la *Loi sur la défense nationale*, le commissaire sera en mesure de traiter plus directement des questions de conformité.

Mes examens des activités entreprises en vertu d'autres autorisations ministérielles en vigueur au cours de l'exercice 2002-2003 étaient en cours à la fin de l'année et feront l'objet de rapports au ministre dans le proche avenir.

Examens d'activités autorisées par le ministre

rapport contient des documents qui nécessitent ce traitement. De fait, je suis heureux de pouvoir dire qu'aucun des examens qui ont formé la base de mes 23 rapports classifiés (y compris les quatre présentés en 2002-2003) n'a fait ressortir de cas d'illégalité ou d'activité non autorisée.

Conformément aux paragraphes 273.65 (1) et (3) de la *Loi sur la défense nationale*, le ministre de la Défense nationale a autorisé par écrit le CST à intercepter des communications privées aux fins d'obtenir des renseignements étrangers et de protéger les systèmes ou les réseaux informatiques de l'État de tout méfait, utilisation non autorisée ou perturbation de leur fonctionnement. Comme nombre des activités exercées en vertu de ces autorisations étaient nouvelles pour le CST, elles ont suscité des défis importants touchant non seulement la technologie, mais aussi des questions comme la détermination des rôles et responsabilités appropriés, l'élaboration d'une politique et de procédures destinées à guider les activités, et l'élaboration de mesures de contrôle afin de garantir le respect des conditions imposées par la loi et par les autorisations ministérielles. Le CST continue de relever ces défis.

L'information fournie par le CST montre que la majeure partie des communications interceptées en vertu de ces autorisations ne sont en fait pas privées (c'est-à-dire qu'il ne s'agit pas de communications de Canadiens). Or je pense que mon examen doit porter uniquement sur les communications privées. Quelles que soient les autres communications interceptées par le CST, c'est l'interception de communications privées qui est autorisée expressément par le ministre. De plus, c'est en ce qui concerne l'interception, l'utilisation et la conservation de communications privées que les questions de légalité et de conformité à l'autorité ministérielle sont le plus susceptibles de se poser.

résultats de chacun de mes examens au ministre au moyen d'un rapport classifié.

La nouvelle loi a apporté certains changements importants à mon mandat. Comme je le mentionne plus haut, le ministre de la Défense nationale peut maintenant autoriser le CST à intercepter les communications privées de Canadiens dans certaines circonstances. Je suis toujours tenu d'examiner les activités du CST en général pour m'assurer qu'elles sont légales, mais la loi m'enjoint en outre expressément d'examiner les activités exercées par le CST en vertu d'autorisations ministérielles pour m'assurer que ces activités sont autorisées, et de faire rapport de cet examen au ministre annuellement.

Autrement dit, je n'ai plus toute latitude pour choisir les sujets d'examen. Mon nouveau mandat défini dans la loi ne m'autorise pas non plus expressément à présenter des rapports renfermant des renseignements classifiés au ministre chaque fois que je le juge à propos. Néanmoins, dans les cas où je choisis les sujets d'examen, j'estime sage de m'en tenir aux pratiques de rapport établies dans le cadre de mon mandat précédent, car elles m'ont bien servi par le passé.

Au cours de l'exercice 2002-2003, j'ai adressé quatre rapports classifiés au ministre, et un autre était presque achevé à la fin de l'année. Il s'agit notamment de rapports exigés par la nouvelle loi et d'examens dont j'avais choisi le sujet. L'annexe C renferme la liste de tous les rapports classifiés que j'ai adressés au ministre depuis ma nomination en 1996.

Comme je l'ai fait remarquer par le passé, la présentation d'un rapport classifié au ministre ne signifie pas que j'aie décelé un manque quelconque de conformité à la loi ou à une autorisation ministérielle. Cela indique simplement que le

ACTIVITÉS DE L'ANNÉE 2002-2003 Rapports classifiés

qu'il fasse rapport annuellement de ces examens au ministre. En me fondant sur mon expérience jusqu'ici, je prévois qu'il s'agira là d'un aspect important et exigeant du rôle du commissaire à l'avenir.

Ce rôle a également été élargi par la *Loi sur la protection de l'information* (ancienne *Loi sur les secrets officiels*). Celle-ci interdit aux personnes astreintes au secret de communiquer ou de confirmer des « renseignements opérationnels spéciaux », y compris ceux qui ont trait aux

activités du CST. Cependant, une personne ne sera pas reconnue coupable d'une infraction si elle peut établir qu'elle a agi dans l'intérêt public. Pour

qu'un juge prenne en considération la « défense d'intérêt public », la personne en cause doit avoir pris une série de mesures prévues dans la loi avant de divulguer l'information. Ces mesures peuvent notamment consister à signaler ses préoccupations relatives aux activités du CST au commissaire et à lui donner un délai raisonnable pour y répondre.

J'ai bon espoir que le commissaire sera rarement appelé à exercer ce rôle, mais celui-ci pourrait être important et risquer d'être exigeant lorsque le cas se présentera.

On trouvera à l'annexe A les dispositions législatives stipulant le mandat du commissaire du Centre de la sécurité des télécommunications.

Conformément aux décrets définissant mon mandat pour la période allant du 19 juin 1996 au 24 décembre 2001, mon bureau a effectué chaque année une série planifiée d'examens des activités du CST. Ces examens ont porté sur des domaines où, à mon avis, la nature même des activités du CST entraînait des risques liés à la légalité. Comme j'étais autorisé à présenter des rapports renfermant des renseignements classifiés au ministre de la Défense nationale chaque fois que je le jugeais à propos, j'ai pris l'habitude de rendre compte des

maintenant l'ampleur, la profondeur et la crédibilité du travail d'examen de mon bureau et en mettant l'accent en particulier sur les questions qui pourraient mettre en danger la vie privée des Canadiens.

Le rôle du commissaire, tel qu'il s'était précisé dans les mandats établis dans les décrets de juin 1996 et de juin 1999 officialisant ma nomination, a été confirmé et élargi par le Parlement en décembre 2001, dans la *Loi antiterroriste*. L'élargissement le plus important découle des dispositions qui permettent au ministre de la Défense nationale d'autoriser l'interception par le CST des communications privées de Canadiens dans des circonstances particulières, sous réserve de l'observance de certaines conditions énoncées dans la loi¹. L'article 183 du *Code criminel* définit une communication privée comme suit :

Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers.

Ce nouveau pouvoir du CST d'intercepter des communications privées lorsque le ministre l'autorise à le faire est un fait nouveau important qui présente des risques manifestes pour la vie privée des Canadiens. La loi reconnaît ces risques et exige notamment que le ministre soit convaincu que le CST a mis en place des mesures adéquates pour protéger celle-ci. Elle prescrit en outre que le commissaire doit examiner les activités exercées en vertu de toutes les autorisations ministérielles pour s'assurer qu'elles sont effectivement autorisées, et

¹ Avant décembre 2001, le CST aurait enfreint les dispositions relatives à la vie privée tant du *Code criminel* que de la *Charte des droits et libertés* s'il avait intercepté des communications sans avoir la certitude que, ce faisant, il n'interceptait pas des communications privées.

électromagnétique et sécurité des technologies de l'information) ainsi que sur certaines autres activités dont il s'acquitte. J'évoque enfin les faits nouveaux qui s'annoncent déjà, et la nomination de mon successeur.

Depuis mon entrée en fonction à titre de commissaire en 1996, le milieu très complexe dans lequel le CST exerce ses activités s'est considérablement transformé. Il en est allé de même de mon bureau et de ce que l'on attend de lui.

ÉVOLUTION DU RÔLE DU COMMISSAIRE

Un des aspects de ce changement touche le contexte à forte composante technologique dans lequel travaille le CST — et la technologie en cause a progressé à un rythme accéléré pendant toute cette période. Un autre élément clé concerne les modifications, du contexte du renseignement découlant de l'évolution des réalités politiques, sociales et économiques. Celles-ci ont entraîné de nouvelles menaces pour la sécurité, la défense et les intérêts nationaux du Canada, et transformé les priorités gouvernementales en matière de renseignement. Pour faire face à ces défis, le CST a élargi son rôle en matière de collecte, d'analyse et de rapports de l'information et des renseignements. Mon personnel et moi-même avons dû nous familiariser avec les technologies complexes en cause et nous tenir au fait des changements rapides qui se produisaient afin de remplir les fonctions d'examen du commissaire d'une manière efficace et efficiente.

Tout au cours de cette période d'évolution technologique rapide qui a marqué le contexte du renseignement et les activités du CST, j'ai suivi le principe selon lequel les Canadiens doivent pouvoir compter que le CST, qui doit nécessairement effectuer la majorité de son travail en secret, le fait en conformité avec les lois du Canada. Ma responsabilité a consisté à leur donner cette assurance, et j'ai cherché à m'en acquitter en

Le présent rapport est mon septième à titre de commissaire du Centre de la sécurité des télécommunications (CST), et le dernier du fait que mon mandat prend fin en juin 2003. C'est par ailleurs la première fois, depuis ma nomination initiale en 1996, que j'ai examiné les activités du CST et rédigé mon rapport annuel dans le cadre d'une loi.

Je signalais dans mon dernier rapport qu'après plus d'une décennie de débats sur le pour et le contre d'une loi habilitante pour le CST, les tragiques événements du 11 septembre 2001 avaient précipité le dépôt et l'adoption par le Parlement de la loi omnibus intitulée *Loi antiterroriste*. Les modifications consécutives apportées à la *Loi sur la défense nationale*, entrées en vigueur le 24 décembre 2001, ont établi un mandat légal pour le CST et pour le commissaire. Les nouvelles dispositions de la *Loi sur la défense nationale* ont inscrit dans celle-ci les activités exercées depuis toujours par le CST et les fonctions que j'exerce depuis 1996, mais elles ont en outre instauré de nouveaux éléments. Ceux-ci sont décrits plus en détail dans la section suivante.

Évaluer les incidences de mes nouvelles responsabilités et commencer à satisfaire aux exigences de la loi ont absorbé une bonne partie de l'année écoulée. Celle-ci a donc été marquée par des défis et des changements tant pour le CST que pour mon bureau, alors que nous sommes efforcés d'arriver à une compréhension commune de nos rôles et responsabilités respectifs.

Dans le présent rapport, je fais une brève rétrospective de l'évolution et du développement du rôle du commissaire au cours des sept dernières années. Je rends également compte des activités d'examen et des constatations faites par mon bureau en 2002-2003. Celles-ci ont porté sur les deux principaux programmes du CST (renseignement

TABLE DES MATIÈRES

Introduction	1
Evolution du rôle du commissaire.....	2
Activités de l'année 2002-2003.....	4
• Rapports classifiés	4
• Examens d'activités autorisées par le ministre.....	6
• Autres examens.....	8
• Constatations faites en 2002-2003.....	10
• Plaintes et préoccupations relatives aux activités du CST.....	11
• Conférence des organismes d'examen.....	11
Le bureau du commissaire.....	11
• Dépenses du bureau et personnel.....	11
• Locaux	12
Coup d'œil sur l'avenir.....	12
• La Loi sur la sécurité publique	12
• Nomination d'un nouveau commissaire.....	13
• Dernières réflexions.....	14
Annexe A : Mandat du commissaire	15
Annexe B : Budget et dépenses, 2002-2003.....	17
Annexe C : Rapports classifiés, 1996-2003	19

4738

Communications Security
Establishment Commissioner

The Honourable Claude Bisson, O.C.



CANADA

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Claude Bisson, O.C.

Juin 2003

L'honorable John McCallum, C.P.
Ministre de la Défense nationale
Edifice Mgen G.R. Pearkes, 13^e étage
101, promenade Colonel By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63 (3) de la *Loi sur la défense nationale*, j'ai le plaisir de vous soumettre mon rapport annuel pour l'année 2002-2003, qui fait état de mes activités et constatations, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

A stylized signature of Claude Bisson, consisting of a large, flowing 'S' shape followed by the name 'Claude Bisson' in a cursive script.
Claude Bisson

P.O. Box/C.P. 1984, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

Bureau du Commissaire du Centre de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044
Télec. : (613) 992-4096

© Ministère des Travaux publics et des Services gouvernementaux Canada 2003
ISBN 0-662-67417-0
N° de cat. D95-2003

Commissaire
du Centre
de la sécurité
des télécommunications



Canada



Rapport annuel

2002
↑
2003

